



『Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics、Release 3.7 (x) 』

初版：2022年3月14日

最終更新：2022年5月1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/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

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

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

© 2022 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	新規および変更情報 1
	新規および変更情報 1

第 2 章	GUI の概要 3
	概要 3
	ダッシュボード 4
	[アプリケーション管理 (Application Management)] > [テナント (Tenants)] ページ 6
	[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] ページ 8
	[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] ページ 9
	[インフラストラクチャ (Infrastructure)] > [サイト (Sites)] ページ 9

第 1 部 :	アプリケーション管理およびファブリック リソース 11
---------	------------------------------------

第 3 章	テナント 13
	テナント 13
	テナントの追加 14

第 4 章	スキーマ 17
	スキーマ設計上の考慮事項 17
	単一スキーマの展開 18
	ネットワーク分離での複数スキーマ 18
	オブジェクトの関係性に基づく複数スキーマ 21
	設定の同時更新 22
	スキーマとテンプレートの作成 24

APIC サイトからのスキーマ要素のインポート	26
VRF の設定	27
ブリッジドメインの設定	28
ブリッジドメインのサイトローカルプロパティの設定	32
アプリケーションプロファイルと EPG の設定	33
EPG のサイトローカルプロパティの設定	35
コントラクトとフィルタの設定	39
オンプレミス外部接続の設定	42
スキーマの表示	44
テンプレート オブジェクトの一括更新	45
サイトへのテンプレートの割り当て	47
テンプレートのバージョンニング	48
タギングテンプレート	49
履歴の表示と以前のバージョンの比較	49
以前の製品バージョンへの復元	52
テンプレートのレビューと承認	53
テンプレート承認要件の有効化	54
必要なロールを持つユーザの作成	54
テンプレートのレビューと承認の要求	55
テンプレートのレビューと承認	56
テンプレートの展開	57
テンプレートの展開解除	61
サイトからのテンプレートの関連付け解除	62
設定のばらつき	63
設定のばらつきの調整	65
スキーマの複製	67
テンプレートの複製	69
テンプレート間でのオブジェクトの移行	71
現在展開されている設定の表示	72
スキーマの概要と展開ビジュアライザ	74
シャドウ オブジェクト	77

APIC GUI でシャドウ オブジェクトを非表示にする 81

第 II 部 :

操作 85

第 5 章

監査ログ 87

監査ログ 87

第 6 章

バックアップと復元 89

設定のバックアップと復元 89

バックアップと復元に関するガイドライン 89

古いローカルバックアップのダウンロードとインポート 92

バックアップのリモート ロケーションの設定 93

バックアップのアップロード 94

バックアップの作成 95

バックアップの復元 96

バックアップのダウンロード 100

バックアップ スケジューラ 101

第 7 章

サイトのアップグレード 103

概要 103

注意事項と制約事項 105

コントローラとスイッチ ノードのファームウェアをサイトにダウンロードする 106

コントローラのアップグレード 108

ノードのアップグレード 110

第 8 章

テクニカル サポート 115

テクニカル サポートおよびシステム ログ 115

システム ログのダウンロード 116

外部アナライザへのストリーミング システム ログ 116

第 III 部 :

インフラストラクチャ管理 121

第 9 章	システム設定 123
	システム設定 123
	システム エイリアスとバナー 123
	ログイン試行回数とロックアウト時間 124

第 10 章	Nexus Dashboard での NDO サービスのアップグレード 125
	概要 125
	前提条件とガイドライン 125
	Cisco App Store を使用した NDO サービスのアップグレード 127
	NDO サービスの手動アップグレード 129
	設定のばらつきの解決とテンプレートの再展開 131

第 11 章	Cisco ACI サイトの設定 137
	ポッドプロファイルとポリシー グループ 137
	すべての APIC サイトのファブリック アクセス ポリシーの設定 138
	ファブリック アクセス グローバル ポリシーの設定 138
	ファブリック アクセス インターフェイス ポリシーの設定 139
	リモート リーフ スイッチを含むサイトの設定 142
	リモート リーフの注意事項と制限事項 142
	リモート リーフ スイッチのルーティング可能なサブネットの設定 142
	リモート リーフ スイッチの直接通信の有効化 143
	Cisco Mini ACI ファブリック 144

第 12 章	サイトの追加と削除 145
	Cisco NDO と APIC の相互運用性のサポート 145
	Cisco ACI サイトの追加 147
	サイトの削除 150
	ファブリック コントローラへの相互起動 151

第 13 章	インフラ一般設定 153
--------	---------------------

第 14 章

Cisco APIC サイトのインフラの設定	161
サイト接続性情報の更新	161
インフラの設定: オンプレミス サイトの設定	162
インフラの設定: ポッドの設定	165
インフラの設定: スパインスイッチ	165

第 15 章

Cisco Cloud APIC サイトのインフラの設定	169
クラウドサイト接続性情報の更新	169
インフラの設定: クラウドサイトの設定	170

第 16 章

ACI サイト向けのインフラ設定の展開	173
インフラ設定の展開	173
オンプレミスとクラウドサイト間の接続の有効化	174

第 17 章

CloudSec 暗号化	179
Cisco ACI CloudSec 暗号化	179
要件と注意事項	180
CloudSec 暗号化に関する用語	183
CloudSec の暗号化と復号の処理	184
CloudSec 暗号化キーの割り当てと配布	187
CloudSec 暗号化のための Cisco APIC の設定	190
GUI を使用した CloudSec 暗号化の Cisco APIC の設定	190
NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定	191
REST API を使用した CloudSec 暗号化の Cisco APIC の設定	192
Nexus Dashboard Orchestrator GUI を使用した CloudSec 暗号の有効化	193
スイッチでの CloudSec 構成の確認	194
スパインスイッチメンテナンス中のキー再生成プロセス	196

NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする 196

REST API を使用したキー再生成プロセスの無効化と再有効化 197

第 IV 部 : 機能と使用例 199

第 18 章 DHCPリレー 201

DHCP リレー ポリシー 201

注意事項と制約事項 202

DHCP リレー ポリシーの作成 203

DHCP オプション ポリシーの作成 204

DHCP ポリシーの割り当て 205

DHCP リレー コントラクトの作成 206

APIC での DHCP リレー ポリシーの確認 208

既存の DHCP ポリシーの編集または削除 208

第 19 章 EPG 優先グループ 211

EPG 優先グループ 211

優先グループに対する EPG の設定 213

第 20 章 サイト内 L3Out 215

サイト間 L3Out の概要 215

サイト内 L3Out のガイドラインと制約事項 216

外部 TEP プールの設定 218

サイト間 L3Out および VRF の作成またはインポート 218

サイト間 L3Out を使用するための外部 EPG の設定 221

サイト間 L3Out のコントラクトの作成 224

使用例 227

アプリケーション EPG のサイト間 L3Out (VRF内) 227

アプリケーション EPG のサイト間 L3Out との共有サービス (Inter-VRF) 231

サイト間中継ルーティング 233

第 21 章

PBR を使用したサイト間 L3Out 237

PBR を使用したサイト間 L3Out 237

サポートされる使用例 238

注意事項と制約事項 242

APIC サイトの設定 243

外部 TEP プールの設定 243

L4-L7 デバイスおよび PBR ポリシーの作成と設定 244

テンプレートの作成 248

サービス グラフの設定 249

コントラクトのフィルタの作成 251

アプリケーション EPG の作成 257

アプリケーション EPG の VRF およびブリッジ ドメインの作成 257

アプリケーション プロファイルと EPG の作成 258

L3Out 外部 EPG の作成 260

サイト間 L3Out および VRF の作成またはインポート 260

外部 EPG の設定 262

第 22 章

レイヤ 3 マルチキャスト 265

レイヤ 3 マルチキャスト 265

レイヤ 3 マルチキャスト ルーティング 266

ランデブー ポイント 267

マルチキャスト フィルタ処理 268

Layer 3 マルチキャストに関するガイドラインと制限事項 269

マルチキャスト ルート マップ ポリシーの作成 271

Any-Source Multicast (ASM) マルチキャストの有効化 272

ソース固有マルチキャスト (SSM) の有効化 274

第 23 章

IPN 全体での QoS の保持 279

QoS およびグローバル DSCP ポリシー 279

DSCP ポリシーの注意事項と制限事項 279

グローバル DSCP ポリシーの設定	280
EPG およびコントラクトの QoS レベルの設定	282

第 24 章**SD-Access と ACI 統合 285**

Cisco SD-Access と Cisco ACI の統合	285
マクロセグメンテーション	286
Cisco SD-Access および Cisco ACI 統合ガイドライン	289
DNA センターのオンボーディング	291
SD Access ドメインへの接続の構成	291
SD Access to ACI 統合のステータスの表示	293
仮想ネットワークの拡張	296
VN の VRF へのマッピングまたはマッピング解除	298
トランジットルーティングの設定	301

第 25 章**SD-WAN の統合 307**

SD-WAN の統合	307
SD-WAN 統合の注意事項と制約事項	308
vManage コントローラの追加	309
グローバル DSCP ポリシーの設定	310
EPG およびコントラクトの QoS レベルの設定	312

第 26 章**SR-MPLS 経由で接続されたサイト 315**

SR-MPLS およびマルチサイト	315
インフラの設定	317
注意事項と制約事項	317
SR-MPLS QoS ポリシーの作成	320
SR-MPLS インフラ L3Out の作成	321
SR-MPLS テナントの要件と注意事項	325
SR-MPLS ルートマップ ポリシーの作成	328
SR-MPLS 設定のテンプレートの有効化	330
VRF および SR-MPLS L3Out の作成	330

サイトローカル VRF 設定の構成	331
サイトローカル SR-MPLS L3Out 設定の構成	332
MPLS ネットワークにより区切られた EPG 間の通信 設定の展開	333 334

第 27 章

vzAny コントラクト	337
vzAny および Multi-Site	337
vzAny およびマルチサイトのガイドラインと制限事項	338
コントラクトとフィルタの作成	340
コントラクトを消費または提供するための vzAny の設定	341
vzAny VRF の一部として EPG を作成する	342
自由な VRF 間通信	343
拡張された EPG	344
サイトローカル EPG	345
サイトローカルおよび拡張 EPG の組み合わせ	346
VRF 内のサイト間 L3Out	347
VRF 間 サイト間 L3Out	348
多対 1 の通信	349
VzAny VRF 内のプロバイダ EPG	350
独自の VRF でのプロバイダ EPG	351



第 1 章

新規および変更情報

- [新規および変更情報 \(1 ページ\)](#)

新規および変更情報

次の表に、このガイドの最初に発行されたリリースから現在のリリースまでに、このガイドの編成と機能に加えられた大幅な変更の概要を示します。テーブルは、ガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

表 1: 最新のアップデート

リリース	新機能またはアップデート	参照先
3.7(1)	このドキュメントの最初のリリース。	--



第 2 章

GUI の概要

- 概要 (3 ページ)
- ダッシュボード (4 ページ)
- [アプリケーション管理 (Application Management)] > [テナント (Tenants)] ページ (6 ページ)
- [アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] ページ (8 ページ)
- [アプリケーション管理 (Application Management)] > [ポリシー (Policies)] ページ (9 ページ)
- [インフラストラクチャ (Infrastructure)] > [サイト (Sites)] ページ (9 ページ)

概要

Nexus Dashboard Orchestrator (NDO) GUI はブラウザ ベースのグラフィカル インターフェイスで、Cisco APIC、クラウド APIC、および DCNM の展開を設定し、監視できます。

GUI は、機能に応じて配置されています。たとえば、[**ダッシュボード (Dashboard)**] ページには、ファブリックとそのヘルスの概要が表示されます。[**サイト (sites)**] ページでは、各サイトに関する情報が提供され、サイトを追加できます。[**スキーマ (schema)**] ページでは、スキーマの作成と設定を行うことができます。各 NDO GUI ページの機能については、次のセクションで説明されています。

各ページの上には、動作しているコントローラの数を示すコントローラステータス、および [**開始 (Get Started)**] メニューアイコン、[**設定**] アイコン、[**ユーザ**] アイコンが示されます。

[**開始 (Get Started)**] メニューは、サイトまたはスキーマの追加、特定のポリシーの設定、管理タスクの実行など、実行する可能性のある多数の一般的なタスクへの簡単なアクセスを提供します。

[**設定 (Settings)**] アイコンを使用すると、現在実行中のバージョン、現在のリリースの最新情報、API ドキュメント、システム ステータスなど、Nexus Dashboard Orchestrator の概要情報にアクセスできます。

- [**NDOについて (About NDO)**] リンクには、現在インストールされている Nexus Dashboard Orchestrator のバージョンに関する情報が表示されます。

- **[このリリースの最新情報 (What's New in This Release)]** リンクをクリックすると、お使いのリリースの新機能の概要や、Nexus Dashboard Orchestrator の他のドキュメントへのリンクが表示されます。
- **[API ドキュメント (API Docs)]** リンクをクリックすると、一連の Swagger API オブジェクトとメソッドの参照にアクセスできます。Swagger API の使用の詳細については、『Cisco ACI Multi-Site REST API 設定ガイド』を参照してください。
- **[システム ステータス (System Status)]** リンクは、NDO で使用されているすべての実行中のサービスのステータスと正常性を提供します。

[ユーザー (User)] アイコンを使用すると、設定やブックマークなど、現在ログインしているユーザーに関する情報を表示できます。また、Orchestrator GUI からログアウトすることもできます。



(注) リリース 3.2 (1) 以降、ユーザ管理は、NDO サービスが実行されている Nexus ダッシュボードの共通ユーザおよび認証管理に移動しました。

- **[設定 (Preferences)]** リンクを使用すると、いくつかの GUI オプションを変更できます。
- **[ブックマーク (Bookmarks)]** リンクをクリックすると、Orchestrator の使用中に保存したすべてのブックマークされたスキーマのリストが開きます。スキーマを表示または編集する際に、画面の右上隅にあるブックマークアイコンをクリックして、スキーマをブックマークすることができます。

ファブリックオブジェクトを使用すると、オブジェクトが表示されるたびに、Orchestrator の GUI 全体で **[表示名 (Display Name)]** フィールドが使用されます。オブジェクトの作成時に表示名を指定できますが、サイトコントローラでのオブジェクトの命名要件により、無効な文字は削除されます。結果として得られた **内部名** が、オブジェクトをサイトにプッシュするときに使用されます。テナントの作成時に使用される **内部名** は、通常、**[表示名 (Display Name)]** テキストボックスの下に表示されます。

ダッシュボード

Nexus Dashboard Orchestrator ダッシュボードには、現在の機能と健全性だけでなく、サイトの実装のすべてのリストが表示されます。

ダッシュボードには次の機能領域があります:

- **サイトのステータス:** サイトのステータスのテーブルには、名前と場所に従ってサイトの一覧が表示されます。このテーブルには、わかりやすいカラーコードによって、実装の現在の健全性も表示されます。
 - **[Controller State]** カラムには、使用可能および実行中のコントローラの数が表示されません。複数サイトの実装では、最大で 3 つのコントローラを設定できます。たとえば、3 つのコントローラのうち 1 つがダウンしている場合には、2/3 として表示されます。

- **[Connectivity]** カラムには、BGP セッションの動作ステータスとデータプレーンユニキャスト、およびダッシュボードの各サイトでピアサイトに接続されているマルチキャストトンネルが示されます。

1 つ以上の BGP セッションまたはトンネル確立に失敗した場合、**Multi-Site** は、BGP セッションまたはトンネル確立に失敗したのがどのローカルスパインとリモートスパインであるかについての情報を提供します。**Multi-Site** は、インフラストラクチャ構成内のサイトを有効にします。ピアサイトへの BGP セッションとデータプレーンユニキャストおよびマルチキャストトンネルが確立されるようにするためです。

BGP セッション

- BGP ピアリングタイプが **Infra-> General Settings** でフルメッシュになっている場合、BGP ピアリングを有効にしたサイトのスパインノードは、すべてのピアサイト内で BGP ピアリングが有効にされているすべてのスパインノードに対して BGP セッションを確立します。
- BGP ピアリングタイプが **Infra-> General Settings**, でルートリフレクタになっている場合、BGP ピアリングとルートリフレクタの両方を有効にしたサイトのスパインノードは、すべてのピアサイト内で BGP ピアリングが有効にされているすべてのスパインノードに対して BGP セッションを確立します。ルートリフレクタモードでは、少なくともローカルスパインノードまたはリモートスパインノードまたはその両方で、ルートリフレクタを有効にする必要があります。そうしないと、それらの間で BGP セッションは確立されません。
- ローカルおよびリモート ASN が異なる場合は、**eBGP** になります。したがって、それらのサイト間のセッションは、BGP ピアリングタイプとルートリフレクタの構成に関係なく、常にフルメッシュとなります。

ユニキャストおよびマルチキャストトンネル: ISN に接続し、インフラストラクチャ構成を持つサイトのスパインノードは、ピアサイトで ISN に接続しているすべてのスパインノードに対してトンネルを確立します。

カラーコードは、次の条件を示します。

- **重大** (赤色)
- **メジャー** (オレンジ色)
- **マイナー** (黄色)
- **警告** (緑色)

色インジケータカラムの番号は、サイトごとの障害の数を示しています。

- **Schema Health:** ロケールと健全性のスキーマの一覧を提供します。
 - 対象のスキーマを検索するには、虫めがねアイコンをクリックし、スキーマ名を入力します。
 - **[+]** 記号をクリックして、サイトへの新しいスキーマの追加を開始できます。

- スキーマの詳細とテンプレートのステータスを表示するには、[スキーマ正常性 (Schema Health)] テーブルのサイト ロケールをクリックします。

Schema Health テーブルはヒートマップタイプの表示になっています。対象としているスキーマの健全性が、色に従って表示されます。2つのカラム (つまり、ロケール) にまたがっているスキーマは、拡大状態であることを示しています。

- 色によって強調表示されたセルをクリックすると、対象とするスキーマにどのようなポリシーが組み込まれているかをより詳細に確認できます。スキーマの詳細ページでは、矢印をクリックしてスキーマビルダーに移動し、対象とするスキーマのポリシーの詳細を更新できます。
- 色分けスライダーを使用すると、健全性をさらにレビューすることが必要なスキーマを、範囲を選択して識別できます。たとえば、スライダーの値を80~100の間に調整することができます。その後、指定した範囲に含まれるスキーマの実装を、付随する [Schema Health] テーブルで表示できます。

[アプリケーション管理 (Application Management)] > [テナント (Tenants)] ページ

マルチサイト **Tenants** ページには、実装を構成しているすべてのテナントが一覧表示されます。

Tenants ページのテーブルには、以下の項目が表示されます:

- テナント名
- 割り当て先サイト
- 割り当て先ユーザ
- 割り当て先スキーマ
- アクション

このページの特徴と機能としては、次のものがあります:

- Name:** テナント名をクリックすると、**Tenant Details** の設定にアクセスできます。**Tenant Details** ページでは、次のセクションの編集や更新を行えます:
 - General Settings:** 必要に応じて、表示名と説明を変更します。
 - Associated Sites:** 対象のテナントと関連付けられているサイトを表示します。
 - Associated Users:** 対象のテナントと関連付けられているユーザを表示します。ユーザ名の隣にあるボックスをオンにすれば、ユーザを対象のテナントと関連付けることができます。

- **Associated Schemas: Associated Schema** の一覧をクリックすると、対象のテナントに関連付けられたスキーマが表示されます。
- **Actions: Actions** の一覧をクリックすると、対象テナントの詳細サイトの編集や、新しいネットワーク マッピングの作成を行えます。



(注) **Delete** を **Actions** ドロップダウンメニューから選択すれば、テナントを削除することができます。

- **Add Tenant: Add Tenant** ボタンをクリックすると、実装内容に既存のテナントを追加できます。それから [Tenant Details] ページでは、テナント名、説明、セキュリティドメイン、および関連付けられているユーザを追加できます。

監査ログ

をクリックして、**監査ログ** にアイコン、**スキーマの追加** スキーマ ページのログの詳細を一覧表示するには、**タブ**。[**監査ログ：テナント リスト (Audit Logs: Tenants List)**] ページが表示されます。

ページの表には、次の詳細情報が表示されます：

- 日付
- アクション
- 詳細
- ユーザ

[**最新 (Most Recent)**] タブをクリックすると、特定の期間の監査ログを選択できます。たとえば、2017 年 11 月 14日から 2017 年 11 月 17日までの範囲を選択し、[**適用 (Apply)**] をクリックすると、この期間の監査ログの詳細が [**監査ログ (Audit Logs)**] ページに表示されます。

[**フィルタ (Filter)**] アイコン ([**最新 (Most Recent)**] タブの隣) をクリックすれば、次のような基準に基づいてログの詳細のフィルタ処理を行うことができます：

- [**ユーザ (User)**]:あるユーザまたはすべてのユーザを選択して [**適用 (Apply)**] をクリックすると、ユーザ名に基づいてログの詳細のフィルタ処理を行えます。
- [**アクション (Action)**]: アクションを選択します。たとえば作成、更新または削除を行って [**適用 (Apply)**] をクリックすると、そのアクションに従ってログの詳細のフィルタ処理を行えます。

詳細については、[テナント \(13 ページ\)](#) の章を参照してください。

[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] ページ

[スキーマ (Schemas)] ページでは、すべての実装に関連付けられているスキーマを一覧表示します。

特定のスキーマを検索するには、虫めがねと関連付けられているフィールドを使用します。スキーマを設定に使用するか、VRF、EPG を持つアプリケーションプロファイル、フィルタおよびコントラクト、ブリッジドメイン、外部 EPG を含むテナントポリシーをインポートします。

スキーマの表では、次の情報が表示されます。

- **名前:** スキーマ名をクリックすると、件名スキーマの設定を表示または更新します。
- **テンプレート:** スキーマに使用されるテンプレートの名前が表示されます。テンプレートは、グループポリシーである ACI コンテキストのプロファイルと同様です。ストレッチオブジェクトまたは特有のオブジェクトのテンプレートを作成することができます。
- **テナント:** 件名スキーマに使用されるテナントの名前が表示されます。
- **アクション:** 関連付けられるスキーマを持つ [アクション] フィールドをクリックして、件名スキーマを編集または削除します。

[スキーマの追加 (Add Schema)] ボタンを使用して新しいスキーマを追加できます。これについては、このドキュメントの後のセクションで詳しく説明します。

監査ログ

をクリックして、**監査ログ** にアイコン、**スキーマの追加** スキーマページのログの詳細を一覧表示するには、タブ。[監査ログ : スキーマ リスト] ページが表示されます。

ページの表には、次の詳細情報が表示されます：

- 日付
- アクション
- 詳細
- ユーザ

[**最新 (Most Recent)**] タブをクリックすると、特定の期間の監査ログを選択できます。たとえば、2017 年 11 月 14 日から 2017 年 11 月 17 日までの範囲を選択し、[**適用 (Apply)**] をクリックすると、この期間の監査ログの詳細が [監査ログ (Audit Logs)] ページに表示されます。

[**フィルタ (Filter)**] アイコン ([**最新 (Most Recent)**] タブの隣) をクリックすれば、次のような基準に基づいてログの詳細のフィルタ処理を行うことができます：

- **[ユーザ (User)]**: あるユーザまたはすべてのユーザを選択して **[適用 (Apply)]** をクリックすると、ユーザ名に基づいてログの詳細のフィルタ処理を行えます。
- **[アクション (Action)]**: アクションを選択します。たとえば作成、更新または削除を行って **[適用 (Apply)]** をクリックすると、そのアクションに従ってログの詳細のフィルタ処理を行えます。

[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] ページ

Nexus Dashboard Orchestrator の **[ポリシー (Policies)]** ページには、ファブリック用に設定したすべてのポリシーが表示されます。

[ポリシー (Policies)] ページには、すべてのポリシーのテーブルとともに、それらのタイプの概要、関連付けられているテナント、説明、および使用方法が表示されます。このページを使用して、新しいポリシーを追加したり、既存のポリシーを編集したりすることができます。

以下のポリシーを設定できます。

- DHCPポリシー ([DHCPリレー \(201 ページ\)](#) 章で説明)。
- MPLS QoSポリシー ([SR-MPLS 経由で接続されたサイト \(315 ページ\)](#) 章で説明)。
- ルート マップ ポリシー ([SR-MPLS 経由で接続されたサイト \(315 ページ\)](#) 章で説明)。
- マルチキャスト ルート マップ ポリシー ([レイヤ 3 マルチキャスト \(265 ページ\)](#) 章で説明)。

[インフラストラクチャ (Infrastructure)] > [サイト (Sites)] ページ

NDO の **[インフラストラクチャ (Infrastructure)] > [サイト (Sites)]** ページには、実装されているすべてのサイトが表示されます。次のようなものがあります。

図 1: マルチサイトの [Sites] ページ

Health	Name	Type	Templates	State	Controller URL
	Fabric-2 Site ID: 65002	DCNM	1	Managed	https://172.25.74.139:4...
	Fabric-3 Site ID: 65003	DCNM	3	Managed	https://172.25.74.139:4...
	Fabric-1 Site ID: 65001	DCNM	1	Managed	https://172.25.74.137:4...

[サイト (Sites)] ページには、次の情報が含まれます。

- **[サイトの正常性 (Site Health)]** は、次の色分けされた識別子に従って、サイトの全体的な正常性のステータスを示します。
 - 重大 (赤色)
 - メジャー (オレンジ色)
 - マイナー (黄色)
 - 警告 (緑色)

- **[サイト名 (Site Name)]** には、サイトの追加時に定義したサイトの表示名が表示されます。
- **[サイトのタイプ (Site Type)]** には、ACI や DCNM などのファブリック タイプが表示されます。
- **[テンプレート (Templates)]** 列には、サイトに関連付けられているテンプレートの数が表示されます。
- **[状態 (State)]** 列は、この特定のファブリックがNDOによって管理されているかどうかを示します。

Nexus Dashboard GUI でサイトとそのプロパティを追加し、管理します。NDO の **[サイト (Sites)]** ページには、Nexus Dashboard GUI で使用可能なすべてのサイトが表示され、NDO で管理する特定のサイトを定義できます。

- **[コントローラ URL (Controller URL)]** 列には、サイトのコントローラのインバンド IP アドレスが表示されます。
- アクションメニュー (...) では、サイトのテナント (ACIファブリックのみ) をインポートしたり、サイトのコントローラ UI を開いたりできます。

特定のサイトをクリックすると、右側の **[プロパティ (Properties)]** サイドバーが開き、サイトに関する追加情報を表示できます。



第 1 部

アプリケーション管理およびファブリック リソース

- テナント (13 ページ)
- スキーマ (17 ページ)



第 3 章

テナント

- [テナント \(13 ページ\)](#)
- [テナントの追加 \(14 ページ\)](#)

テナント

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、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。

テナントを管理するには、パワー ユーザまたはサイトとテナント マネージャの読み取り/書き込みロールのいずれかが必要です。

次の 3 つのテナントが事前に設定されています。

- `common` : ACI ファブリックの他のテナントに「共通」のサービスを提供するための特別なテナント。共通テナントの基本原則はグローバルな再利用です。一般的なサービスには、共有 L3Out、DNS、DHCP、Active Directory、共有プライベートネットワークまたはブリッジドメインなどがあります。
- `dcnm-default-tn` : Cisco DCNM ファブリックの設定を提供する特別なテナント。
- `infra` : トンネルやポリシー展開など、ファブリック内部の通信に使用されるインフラストラクチャテナント。これには、スイッチ間の切り替えと APIC 通信への切り替えが含まれます。`infra` テナントは、ユーザー空間 (テナント) には公開されず、独自のプライベートネットワーク空間とブリッジドメインを備えています。ファブリックの検出、イメージ管理、ファブリック機能用の DHCP は、すべてこのテナント内で処理されます。

Nexus Dashboard Orchestrator を使用して Cisco DCNM ファブリックを管理する場合は、事前に設定されているデフォルトの `dcnm-default-tn` を使用し、次のオブジェクトを作成および管理できます。

- VRF

- ネットワーク

テナントの追加

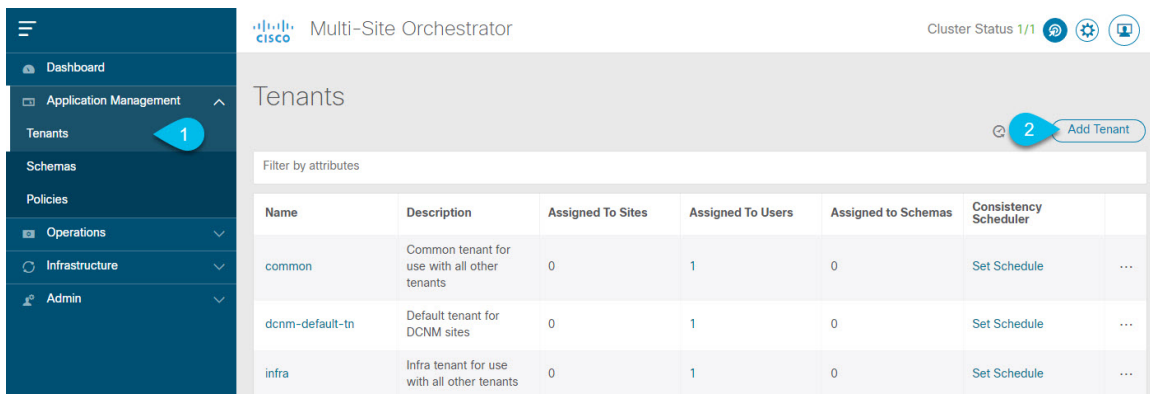
このセクションでは、Nexus Dashboard Orchestrator GUI を使用してテナントを追加する方法について説明します。

始める前に

テナントの作成および管理には、パワー ユーザまたはサイト マネージャの読み取り/書き込みロールを持つユーザが必要です。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 テナントを追加します。



- 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [テナント (Tenants)] を選択します。
- メインペインの右上にある [テナントの追加 (Add Tenant)] をクリックします。
[テナントの追加 (Add Tenant)] 画面が開きます。

ステップ 3 テナントの詳細を入力します。

- [表示名 (Display Name)] とオプションの [説明 (Description)] を入力します。

Orchestrator の GUI 全体で、テナントが表示されるたびに、テナントの表示名が使用されます。ただし、APICでのオブジェクトの命名要件により、無効な文字は削除され、その結果として得られた内部名が、サイトにテナントをプッシュするときに使用されます。テナントの作成時に使用される内部名は、[表示名 (Display Name)] テキストボックスの下に表示されます。

テナントの表示名はいつでも変更できますが、テナントの作成後に内部名を変更することはできません。

- [関連付けられたサイト (Associated Sites)] セクションで、このテナントに関連付けるすべてのサイトと、使用する [セキュリティドメイン (Security Domain)] をオンにします。

選択したサイトのみが、このテナントを使用している任意のテンプレートで使用可能になります。

セキュリティ ドメインは APIC GUI を使用して作成し、アクセスをコントロールするために、さまざまな APIC ポリシーに割り当てることができます。詳細については、*Cisco APIC 基本設定ガイド*を参照してください。

- c) **[関連付けられたユーザー (Associated Users)]** セクションで、テナントへのアクセスが許可されている Nexus Dashboard Orchestrator ユーザーを選択します。

テンプレートを作成するときに選択したユーザのみが、このテナントを使用できます。

- d) (オプション) 整合性チェッカ スケジューラを有効にします。

これにより、定期的な整合性チェックを有効にできます。整合性チェッカ機能の詳細については、*Cisco Multi-Site Troubleshooting Guide* を参照してください。

ステップ 4 [保存 (Save)] をクリックして、テナントの追加を終了します。



第 4 章

スキーマ

- スキーマ設計上の考慮事項 (17 ページ)
- 設定の同時更新 (22 ページ)
- スキーマとテンプレートの作成 (24 ページ)
- テンプレート オブジェクトの一括更新 (45 ページ)
- サイトへのテンプレートの割り当て (47 ページ)
- テンプレートのバージョンニング (48 ページ)
- テンプレートのレビューと承認 (53 ページ)
- テンプレートの展開 (57 ページ)
- テンプレートの展開解除 (61 ページ)
- サイトからのテンプレートの関連付け解除 (62 ページ)
- 設定のばらつき (63 ページ)
- スキーマの複製 (67 ページ)
- テンプレートの複製 (69 ページ)
- テンプレート間でのオブジェクトの移行 (71 ページ)
- 現在展開されている設定の表示 (72 ページ)
- スキーマの概要と展開ビジュアライザ (74 ページ)
- シャドウ オブジェクト (77 ページ)

スキーマ設計上の考慮事項

スキーマは、ポリシーの定義に使用されるテンプレートの集合であり、各テンプレートは特定のテナントに割り当てられます。展開の使用例に固有のスキーマとテンプレートの設定を作成する際に、複数のアプローチを実行できます。ここでは、マルチサイト環境でスキーマ、テンプレート、およびポリシーを定義する方法を決定する際に実行できる、いくつかの簡単な設計方針について説明します。

スキーマを設計するには、スキーマ、テンプレート、およびスキーマあたりのオブジェクトの数に対してサポートされているスケーラビリティ制限を考慮する必要があることに注意してください。検証済みスケーラビリティ制限の詳細については、お使いのリリースの『[Cisco Multi-Site Verified Scalability Guides](#)』を参照してください。

単一スキーマの展開

スキーマ設計の最も簡単なアプローチは、単一のスキーマで単一のテンプレートを導入することです。単一のテンプレートを含む単一のスキーマを作成し、そのテンプレートにすべてのVRF、ブリッジドメイン、EPG、コントラクト、およびその他の要素を追加して、1つまたは複数のサイトに展開することができます。

Multi-Site スキーマを作成する最も簡単な方法は、同じスキーマとテンプレート内にすべてのオブジェクトを作成することです。ただし、サポートされているスキーマの数に制限があるため、このアプローチは大規模な展開に適していない場合があります。これは、これらの制限を超える可能性があります。

また、このアプローチでは、テンプレートで定義されたすべてのオブジェクトが「ストレッチオブジェクト」になり、テンプレートに加えられたすべての変更が、そのようなテンプレートに関連付けられたすべてのサイトに常に同時に展開されることに注意してください。

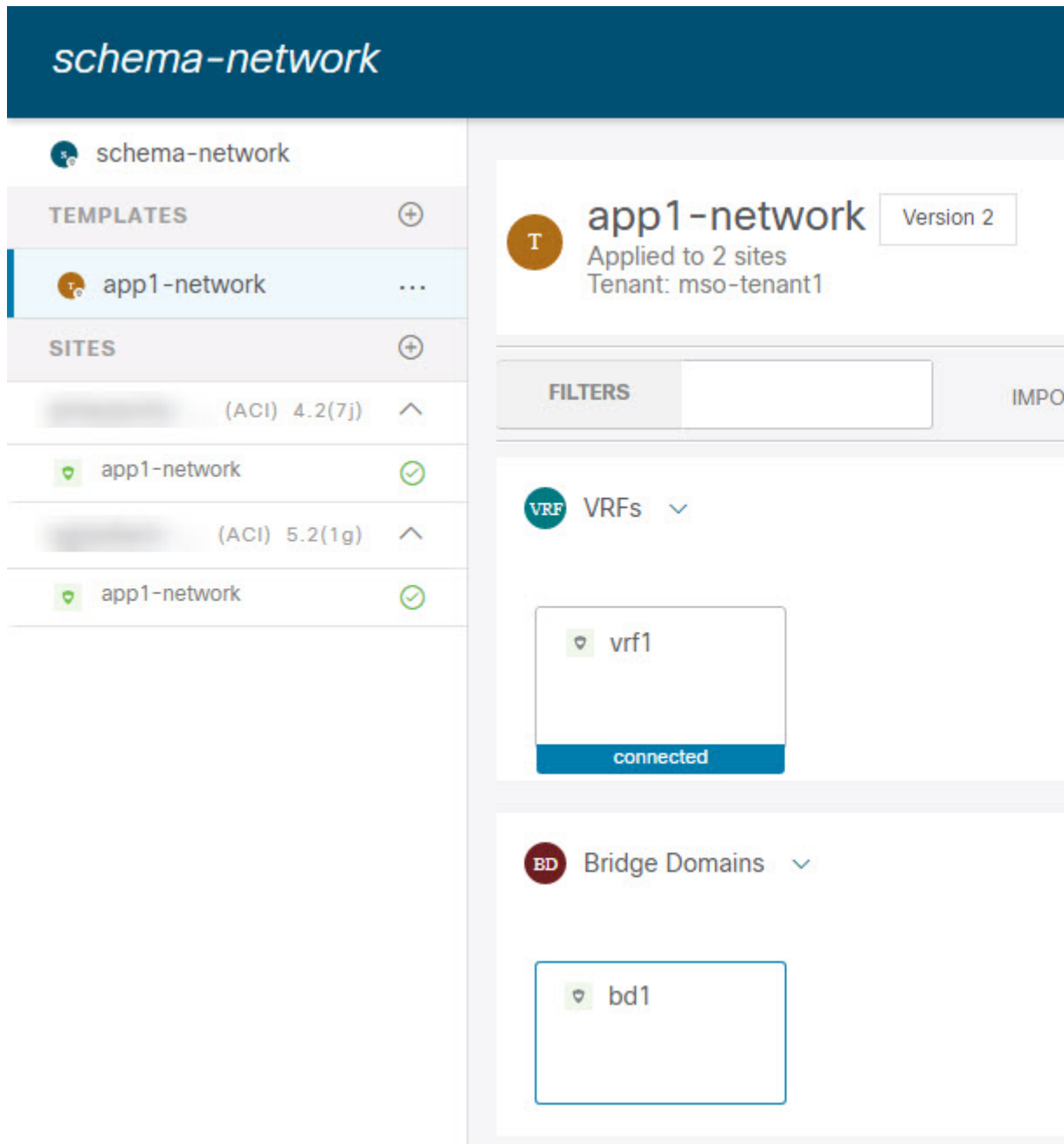
ネットワーク分離での複数スキーマ

スキーマ設計のもう1つのアプローチは、ネットワーク オブジェクトをアプリケーション ポリシー設定から分離することです。ネットワーク オブジェクトには、VRF、ブリッジドメイン、サブネットなどがあり、アプリケーションポリシーオブジェクトには EPG、コントラクト、フィルタ、外部 EPG、およびサービス グラフが含まれます。

最初に、ネットワーク要素を含むスキーマを定義します。すべてのネットワーク要素を含む単一のスキーマを作成するか、または、それらを参照するアプリケーション、またはネットワークが拡張するサイトに基づいて、複数のスキーマに分割します。

次の図は、VRF、BD、およびサブネットが設定され、2つのサイトに展開されている単一のネットワークングテンプレート設定を示しています。

図 2: ネットワーク スキーマ



その後、各アプリケーションのポリシーオブジェクトを含む、1つ以上の個別のスキーマを定義します。この新しいスキーマは、前のスキーマで定義されたブリッジドメインなどのネットワーク要素を参照できます。次の図に、2つのアプリケーションテンプレートを含むポリシースキーマを示します。これらのテンプレートの両方が外部スキーマのネットワーク要素を参照しています。アプリケーションの一方は1つのサイトにローカルであり、他方は2つのサイト間で拡張されます。

図 3: ポリシー スキーマ

The screenshot displays the configuration page for a policy schema named 'schema-policy'. The interface is divided into a left sidebar and a main content area. The sidebar shows a hierarchy of 'TEMPLATES' and 'SITES'. Under 'SITES', two ACI versions are listed: (ACI) 4.2(7j) and (ACI) 5.2(1g). The 'app1-policy' is selected under the (ACI) 5.2(1g) site. The main content area shows the details for 'app1-policy' in the 'mso-tenant1' tenant. It includes sections for 'Application Profile app1', 'EPGs' (with 'app1-db' and 'app1-web' listed), and 'Contracts' (with 'app1-contrast' listed and a 'consumed' status bar).

ポリシースキーマとテンプレートを作成して展開すると、ネットワークスキーマのネットワークキミングオブジェクトに、ポリシースキーマ要素による外部参照の数が表示されます。外部参

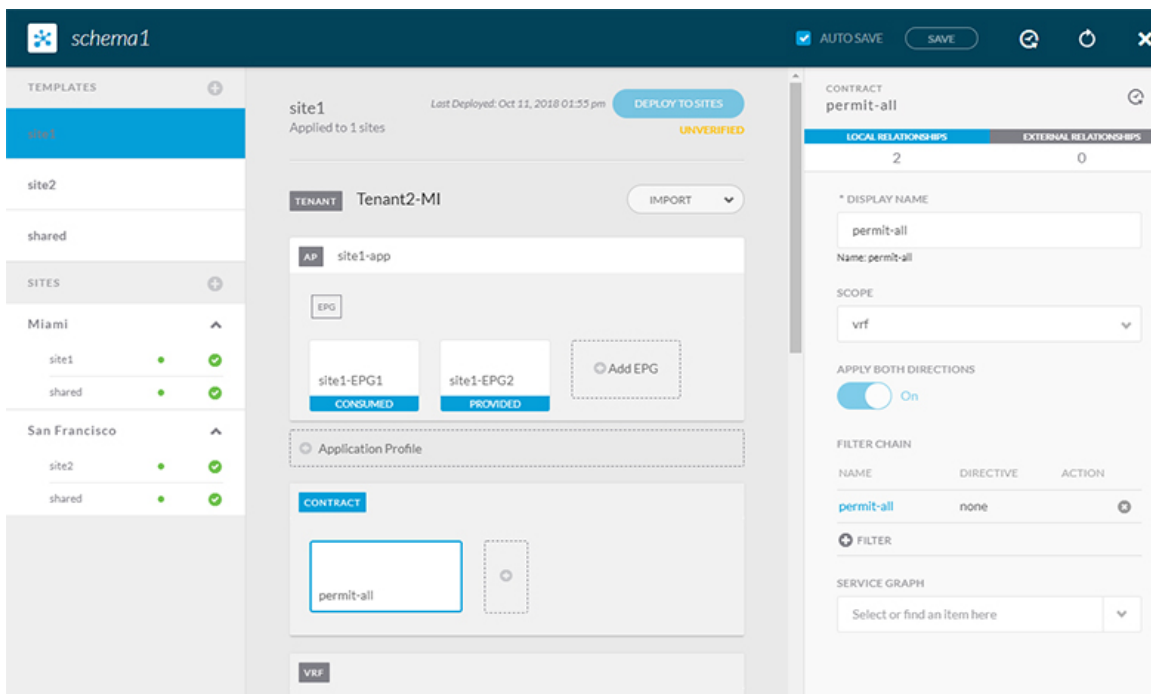
照を含むオブジェクトは、上のネットワークスキーマの図に示すように、リボンのアイコンでも示されます。

この方法で設計されたスキーマは、ネットワーキング オブジェクトをポリシー オブジェクトから論理的な分離します。ただし、これにより、各スキーマで外部参照されたオブジェクトの追跡はさらに複雑になります。

オブジェクトの関係性に基づく複数スキーマ

共有オブジェクト参照を使用して複数のスキーマを設定する場合、それらのオブジェクトを変更する際に注意を払うことが大切です。たとえば、共有ネットワークオブジェクトを変更または削除すると、1つ以上のサイトのアプリケーションに影響を与える可能性があります。そのため、サイトとそのアプリケーションで使用されているオブジェクト (VRF、BD、EPG、コントラクト、フィルタなど) のみを含む、個々のサイトのためのテンプレートを作成するのがよいでしょう。それから、共有オブジェクトを含む別のテンプレートを作成します。

図 4: サイトごとに1つのテンプレート



上の図の **site1** テンプレートには、Site1 に対してローカルなオブジェクトのみが含まれています。このテンプレートは、Miami サイトにのみ展開されます。同様に、**site2** テンプレートには Site2 に関連するオブジェクトのみが含まれており、San Francisco サイトに展開されます。これらのテンプレートのいずれかのオブジェクトに変更を加えても、他のテンプレートのオブジェクトには影響しません。共有テンプレートには、サイト間で共有されるオブジェクトが含まれています。

このシナリオは、次のテンプレート レイアウトを持つ追加サイトに拡張できます。

- サイト 1 テンプレート

- サイト 2 テンプレート
- サイト 3 テンプレート
- サイト 1 と 2 の共有テンプレート
- サイト 1 と 3 の共有テンプレート
- サイト 2 と 3 の共有テンプレート
- すべての共有テンプレート

同様に、展開されているサイトに基づいてオブジェクトを分離するのではなく、個々のアプリケーションに基づいてスキーマとテンプレートを作成することもできます。これにより、各アプリケーションプロファイルを簡単に特定し、それらをスキーマとサイトにマッピングし、さらには各アプリケーションをローカルまたは拡張されたサイト全体のものとして設定することができます。

ただし、これはスキーマごとのテンプレート数の制限（使用しているリリースの [Verified Scalability Guide](#) に記載）をすぐに越えてしまう可能性があるため、複数の組み合わせに対応するために追加のスキーマを作成することが必要になります。これにより、複数のスキーマとテンプレートが追加され、さらに複雑になりますが、サイトまたはアプリケーションに基づいてオブジェクトを正確に分離できます。

設定の同時更新

Nexus ダッシュボード オーケストレータ GUI は、同じサイトまたはスキーマオブジェクトでの同時更新が意図せずに相互に上書きされることがないようにします。自分が開いた後に別のユーザーによって更新されたサイトまたはテンプレートに変更を加えようと、GUI はそれ以降の変更を拒否し、追加の変更を行う前にオブジェクトを更新するように求める警告を表示します。テンプレートを更新すると、その時点までに行った編集内容は失われるため、再度変更する必要があります。



ただし、既存のアプリケーションとの下位互換性を維持するために、デフォルトの REST API 機能は変更されていません。つまり、UI はこの保護を常に有効にしていますが、設定変更を追跡するためには、NDO の API コールに対しても明示的に有効にする必要があります。



(注) この機能を有効にする場合は、次の点に注意してください。

- このリリースでは、サイトオブジェクトとスキーマオブジェクトの競合する設定変更の検出のみがサポートされています。
- PUT および PATCH API コールのみがバージョンチェック機能をサポートします。
- API コールでバージョンチェックパラメータを明示的に有効にしていない場合、NDO は内部的に更新を追跡しません。その結果、設定の更新は、後続の API コールまたは GUI ユーザの両方によって上書きされる可能性があります。

設定のバージョンチェックを有効にするには、使用している API エンドポイントの末尾に `enableVersionCheck = true` パラメータを追加して、API コールにこのパラメータを渡します。次の例をご覧ください。

```
https://<mso-ip-address>/mso/api/v1/schemas/<schema-id>?enableVersionCheck=true
```

例

スキーマ内のテンプレートの表示名を更新する簡単な例を使用して、PUT または PATCH コールでバージョンチェック属性を使用する方法を示します。

最初に、変更するスキーマを GET します。これにより、コールの応答で現在の最新バージョンのスキーマが返されます。

```
{
  "id": "601acfed38000070a4ee9ec0",
  "displayName": "Schema1",
  "description": "",
  "templates": [
    {
      "name": "Template1",
      "displayName": "current name",
      [...]
    }
  ],
  "updateVersion": 12,
  "sites": [...]
}
```

次に、リクエスト URL に、2つの方法のいずれかで、`enableVersionCheck = true` を追加して、スキーマを変更します。



(注) ペイロードの `_updateVersion` フィールドの値が、元のスキーマで取得した値と同じであることを確認する必要があります。

- PUT API を使用して、更新されるスキーマ全体ペイロードとします。

```
PUT /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
{
  "id": "601acfed38000070a4ee9ec0",
```

```

    "displayName": "Schema1",
    "description": "",
    "templates": [
      {
        "name": "Template1",
        "displayName": "new name",
        [...]
      }
    ],
    "_updateVersion": 12,
    "sites": [...]
  }

```

- PATCH API 操作のいずれかを使用して、スキーマ内のオブジェクトの 1 つに特定の変更を加えます。

```

PATCH /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
[
  {
    {
      "op": "replace",
      "path": "/templates/Template1/displayName",
      "value": "new name",
      "_updateVersion": 12
    }
  }
]

```

リクエストが行われると、API は現在のスキーマバージョンを 1 ずつ増やし（12 から 13 など）、新しいバージョンのスキーマの作成を試みます。（enableVersionCheck が有効で）新しいバージョンがまだ存在しない場合、操作は成功し、スキーマは更新されます。別の API コールまたは UI がその間にスキーマを変更していた場合、操作は失敗し、API コールは次の応答を返します。

```

{
  "code": 400,
  "message": "Update failed, object version in the DB has changed, refresh your client and retry"
}

```

スキーマとテンプレートの作成

始める前に

- 管理者ユーザ アカウント（完全な読み取り/書き込み権限を持つ）が必要です。
- テナント アカウント（テナント ポリシーの読み取り/書き込み権限を持つ）が必要です。
Cisco APIC Basic Configuration Guide の *User Access, Authentication, and Accounting* を参照してください。
- サイトに組み込むには、少なくとも 1 つの使用可能なテナントが必要です。
詳細については、[テナントの追加（14 ページ）](#) を参照してください。

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ2 スキーマを新規作成します。

- a) 左側のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。
- b) [スキーマ (Schema)] ページで、[スキーマの追加 (Add Schema)] をクリックします。
- c) スキーマ作成ダイアログで、スキーマの [名前 (Name)] と説明 (オプション) を入力します。

デフォルトでは、新しいスキーマは空であるため、1 つ以上のテンプレートを追加する必要があります。

ステップ3 テンプレートを作成します。

- a) 左側のサイドバーの [テンプレート (Templates)] で、[+] 記号をクリックして新しいテンプレートを追加します。
- b) [テンプレートタイプの選択 (Select a Template type)] ウィンドウで、テンプレートタイプとして [ACI マルチクラウド (ACI Multi-Cloud)] を選択します。

- **ACI マルチクラウド**—Cisco ACI オンプレミスおよびクラウドサイトに使用されるテンプレート。これにより、複数のサイト間でテンプレートとオブジェクトを拡張できます。

次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。

- **ネットワークング (Networking)** — Cisco Nexus ダッシュボードファブリックコントローラ (以前のデータセンター ネットワーク マネージャ) サイト用に設計されたテンプレート。

このガイドでは、Cisco ACI およびクラウド ACI サイトの Nexus Dashboard Orchestrator 構成について説明しました。Cisco NDFC サイトの操作については、代わりに『[Cisco Nexus Dashboard Orchestrator Configuration Guide for DCNM Fabrics](#)』を参照してください。

- **SR-MPLS**—SR-MPLS 統合用に設計されたテンプレート。

SR-MPLS の使用例の詳細については、このガイドの「SD-WAN 統合」の章を参照してください。

- **Cloud Local** — Google Cloud サイト接続など、特定の Cisco Cloud ACI ユースケース向けに設計されたテンプレートであり、複数のサイト間で拡張することはできません。

- c) 右側のサイドバーで、[表示名 (Display name)] を指定します。
- d) (任意) [説明 (Description)] を入力します。
- e) SR-MPLSテンプレートを設定する場合は、**SR-MPLS** ノブを有効にします。

SR-MPLSテンプレートの詳細については、[SR-MPLS 経路で接続されたサイト \(315 ページ\)](#) を参照してください。

- f) [テナントの選択 (Select a Tenant)] ドロップダウンから、このテンプレートのテナントを選択します。

新しいスキーマを作成するために使用しているユーザアカウントは、そのスキーマに追加しようとしているテナントに関連付けられている必要があることに注意してください。そうしないと、テナントはドロップダウンメニューで使用できなくなります。ユーザアカウントとテナントの関連付けについては、[テナントの追加 \(14 ページ\)](#) を参照してください。

ステップ4 テンプレートをサイトに割り当てます。

一度に 1 つのテンプレートを展開するため、設定を展開する少なくとも 1 つのサイトにテンプレートを関連付ける必要があります。

- a) 左側のペインで、サイトの横にある **[+]** のアイコンをクリックします。
- b) **[サイトの追加 (Add Sites)]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。
- c) 各サイトの横にある **[テンプレートに割り当て (Assign to Template)]** ドロップダウンから、1 つ以上のテンプレートを選択します。

テンプレートの展開は、関連付けられているすべてのサイトに一度に 1 つずつ行いますが、サイトへの関連付けは、一度に複数のテンプレートで行えます。

- d) **[保存 (Save)]** をクリックします。

APIC サイトからのスキーマ要素のインポート

新しいオブジェクトを作成し、1 つまたは複数のサイトに公開できます。または、サイトローカルの既存のオブジェクトをインポートし、マルチサイト Orchestrator を使用して管理できます。ここでは、1 つ以上の既存のオブジェクトをインポートする方法について説明します。このドキュメントでは、新しいオブジェクトを作成する方法について説明します。

APIC から NDO にポリシーをインポートする際の一般的な方法は、VRF やコントラクトなどの一部のオブジェクトをストレッチテンプレートにインポートし、その他のオブジェクト（非ストレッチ EPG や BD など）をサイトローカルテンプレートにインポートすることです。

リリース 3.1(1) より前は、ストレッチテンプレートの一部である別のオブジェクトを参照するサイトローカルテンプレートにオブジェクトをインポートすると、次のような特定の問題がありました。

- 参照オブジェクトがすでに NDO に存在し、**[関係を含める (Include Relationships)]** オプションを有効にして新しいオブジェクトをインポートすると、参照オブジェクトがすでに存在するため、オブジェクトの重複が原因で NDO がエラーをスローします。
- ただし、参照オブジェクトをインポートしない場合 (**[関係を含める (Include Relationships)]** オプションが無効になっている場合)、管理者はインポート後に参照オブジェクトとの手動マッピングを実行する必要があります。

リリース 3.1(1) 以降では、（同じまたは異なるスキーマ内の）異なるテンプレートの一部である別のオブジェクトとの参照を持つサイトローカルテンプレートにオブジェクトをインポートすると、参照は NDO によって自動的に解決されます。このような場合、インポートされているオブジェクトの UI で **[関係をインポート (Import Relationships)]** オプションがグレー表示され、**[参照されたオブジェクト (Referenced Object)]** が **[テンプレート (Template)]** にすでに存在するなどの追加情報が提供されます。既存の関係はデフォルトでインポートされます。このようなオブジェクトはデフォルトで関係とともにインポートされますが、インポート操作が完了したら、BD を別の VRF に再マッピングするなどして、参照を変更できます。新しい動作は、インポート可能なすべての設定オブジェクトに適用されます。

サイトから 1 つ以上のオブジェクトをインポートするには、次の手順を実行します。

-
- ステップ 1** [スキーマ (Schema)] ページで、オブジェクトをインポートするスキーマを選択します。
- ステップ 2** 左側のサイドバーで、オブジェクトをインポートするテンプレートを選択します。
- ステップ 3** メインペインで[インポート (Import)] ボタンをクリックし、インポート元の[サイト (Site)] を選択します。
- ステップ 4** [インポート元 (Import from)] <site-name> ウィンドウが開いたら、インポートするオブジェクトを 1 つまたは複数選択します。

(注) NDO にインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

- ステップ 5** (オプション) [関係のインポート (Import relations)] ノブを有効にして、すべての関連オブジェクトをインポートします。

たとえば、BD をインポートする場合、[関係のインポート (Import Relationships)] ノブを有効にすると、関連する VRF もインポートされます。

(注) 前述したように、関連オブジェクトがすでに NDO に存在するオブジェクトに対しては、[関係のインポート (Import Relationships)] ノブはデフォルトで有効になり、無効にできません。

VRF の設定

このセクションでは、VRF の設定方法を説明します。

始める前に

[スキーマとテンプレートの作成 \(24 ページ\)](#) の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

-
- ステップ 1** VRF を作成するためのスキーマとコントラクトを選択します。
- メインペインで、[+ オブジェクトの作成 (+Create Object)] > [VRF] を選択します。
または、[VRF] エリアまでスクロールダウンし、タイルの上にマウスを移動して、[VRF の追加 (Add VRF)] をクリックします。
 - 右側のペインで、VRF の [表示名 (Display Name)] を入力します。
 - (任意) [説明 (Description)] を入力します。
- ステップ 2** VRF の [オンプレミス プロパティ (On-Premises Properties)] を設定します。
- [ポリシー制御適用の選択 (Policy Control Enforcement Preference)] を指定します。
新しく作成された VRF のポリシー制御の適用は変更できず、設定は適用モードにロックされます。

ただし、これを使用して、インポート後、非適用として設定されている APIC サイトからインポートした VRF を適用モードに移行することができます。一般的な使用例は、既存の VRF を強制モードに変換してサイト間での拡張をサポートする必要がある、ブラウンフィールド展開です。インポートした VRF を NDO で非適用から適用に移行すると、このフィールドをさらに変更することはできなくなります。

- [適用 (Enforced)] : セキュリティルール (コントラクト) が適用されます。
- [非適用 (Unenforced)] : セキュリティルール (コントラクト) は適用されません。

- b) (任意) **[IPデータプレーン学習 (IP Data-Plane Learning)]** を有効にします。

IP アドレスが VRF のデータプレーン パケットを通じて学習されるかどうかを定義します。

無効の場合、IP アドレスはデータプレーン パケットから学習されません。ローカルおよびリモート MAC アドレスは学習されますが、ローカル IP アドレスはデータ パケットから学習されません。

このパラメータが有効か無効かに関係なく、ローカル IP アドレスは ARP、GARP、および ND から学習できます。

- c) (オプション) VRF の **[レイヤ 3 マルチキャスト (L3 Multicast)]** を有効にします。

詳細については、[レイヤ 3 マルチキャスト \(265 ページ\)](#) を参照してください。

- d) (オプション) VRF の **[vzAny]** を有効にします。

詳細については、[vzAny コントラクト \(337 ページ\)](#) を参照してください。

ブリッジドメインの設定

このセクションでは、ブリッジドメイン (BD) を設定する方法について説明します。

始める前に

- [スキーマとテンプレートの作成 \(24 ページ\)](#) の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。
- [VRF の設定 \(27 ページ\)](#) の説明に従って VRF を作成する必要があります。

ステップ 1 ブリッジドメインを作成するためのスキーマとコントラクトを選択します。

ステップ 2 ブリッジドメインを作成します。

- メインペインで、**[+オブジェクトの作成 (+Create Object)]** > **[ブリッジドメイン (Bridge Domains)]** を選択します。

または、**[ブリッジドメイン (Bridge Domains)]** エリアまでスクロールダウンし、タイルの上にマウスを移動して、**[ブリッジドメインの追加 (Add Bridge Domains)]** をクリックします。
- 右側のペインで、ブリッジドメインの **[表示名 (Display Name)]** を入力します。
- (任意) **[説明 (Description)]** を入力します。

ステップ 3 [オンプレミス プロパティ (On-Premises Properties)] を設定します。

- a) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、ブリッジドメインを選択します。
- b) (オプション) **[L2 ストレッチ(L2 Stretch)]** を有効にします。
- c) (オプション) **[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)]** を有効にします。
このオプションは、**L2 ストレッチ**を有効にした場合に使用可能になります。
- d) (オプション) **[最適化された WAN 帯域幅 (Optimized WAN Bandwidth)]** を有効にします。
- e) (オプション) **[ユニキャスト ルーティング (Unicast Routing)]** を有効にします。

この設定が有効で、サブネットアドレスが構成されている場合、ファブリックがデフォルト ゲートウェイ機能を提供し、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP 学習は、ブリッジドメイン内にサブネットが構成されているかどうかにかかわらず行われます。

- f) (オプション) BD の **[L3 マルチキャスト (L3 Multicast)]** を有効にします。

Layer 3 マルチキャストの詳細については、[レイヤ 3 マルチキャスト \(265 ページ\)](#) を参照してください。

- g) (オプション) **[L2 不明なユニキャスト (L2 Unknown Unicast)]** モードを選択します。

デフォルトでは、ユニキャストのトラフィックは、レイヤ 2 ポートに対してフラッディングされません。該当する場合、特定のポートでユニキャストトラフィックフラッディングがブロックされ、ポート上に存在する既知の MAC アドレスを持つ出力トラフィックのみが許可されます。可能な方式は [フラッディング (Flood)] または [ハードウェア プロキシ (Hardware Proxy)] です。

BD が L2 Unknown Unicast を持っており、それが Flood に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカルリーフスイッチから削除します。そして、**Clear Remote MAC Entries** を選択すると、BD が展開されているリモートのリーフスイッチからも削除されます。この機能を使用しない場合、リモートリーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。

(注) L2 Unknown Unicast の設定を変更すると、このブリッジドメインに関連付けられた EPG にアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします(アップダウンします)。

- h) (オプション) **[不明なマルチキャストフラッディング (Unknown Multicast Flooding)]** モードを選択します。

これは、IPv4 の不明マルチキャストトラフィックに適用される、レイヤ 3 不明マルチキャスト宛先のノード転送パラメータです。

- [フラッド (Flood)] (デフォルト) : 不明な IPv4 マルチキャストトラフィックは、このブリッジドメインに関連付けられた EPG に接続されたすべての前面パネルポートでフラッディングされます。フラッディングは、ブリッジドメインの M ルータポートだけに制限されません。
- [フラッドの最適化 (Optimize Flood)] : ブリッジドメイン内の M ルータポートにのみデータを送信します。

- i) (オプション) **[IPv6 不明マルチキャスト フラッディング (IPv6 Unknown Multicast Flooding)]** モードを選択します。
- これは、IPv6不明マルチキャストトラフィックに適用される、レイヤ3不明マルチキャスト宛先のノード転送パラメータです。
- [フラッド (Flood)] (デフォルト) : 不明な IPv6 マルチキャストトラフィックは、このブリッジドメインに関連付けられたすべての前面パネルポートでフラッディングされます。フラッディングは、ブリッジドメインの M ルータポートだけに制限されません。
 - [フラッドの最適化 (Optimize Flood)] : ブリッジドメイン内の M ルータポートにのみデータを送信します。
- j) (オプション) **[複数宛先フラッディング (Multi-Destination Flooding)]** モードを選択します。
- レイヤ 2 マルチキャストおよびブロードキャストトラフィックの複数宛先転送方式です。
- [BD のフラッド (Flood in BD)] : 同じブリッジドメイン上のすべてのポートにデータを送信します。
 - [ドロップ (drop)] : パケットをドロップします。他のポートにデータを送信しません。
 - [カプセル化のフラッド (Flood in Encapsulation)] : ブリッジドメイン全体にフラッディングされるプロトコルパケットを除き、ブリッジドメイン内の同じ VLAN を持つすべての EPG ポートにデータを送信します。
- (注) このモードは、**[L2 ストレッチ (L2 Stretch)]** オプションが無効になっている場合にのみサポートされ、サイト間でストレッチされる BD ではサポートされません。
- k) (オプション) **[ARP フラッディング (ARP Flooding)]** を有効にします。
- これによって ARP フラッディングが有効になり、レイヤ 2 ブロードキャストドメインが IP アドレスを MAC アドレスにマッピングします。フラッディングがディセーブルである場合、ユニキャストルーティングはターゲット IP アドレスで実行されます。
- ARP 要求がレイヤ 2 ブロードキャストドメイン内でフラッディングされるように、ARP フラッディングを有効にします。BD がサイト間で拡張されている場合、ARP フラッディングを有効にできるのは、**[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)]** を有効にした場合のみです。ARP フラッディングが無効な場合、ローカルに接続されたエンドポイントから ARP 要求を受信するリーフは、ARP 要求のターゲットエンドポイントが接続されているリモートリーフに直接転送するか (リモートエンドポイントの IP がエンドポイントテーブルで既知の場合)、またはスパインへ転送します (リモートエンドポイントの IP がエンドポイントテーブルで不明な場合)。
- [L2 不明なユニキャスト (L2 Unknown Unicast)]** モードを [フラッド (Flood)] に設定した場合、**[ARP フラッディング (ARP Flooding)]** は無効にできません。**[L2 不明なユニキャスト (L2 Unknown Unicast)]** モードを [ハードウェア プロキシ (Hardware Proxy)] に設定した場合、ARP フラッディングは有効または無効にできます。
- l) (オプション) **[仮想 MAC アドレス (Virtual MAC Address)]** を入力します。

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

(注) 仮想MACと仮想IPサブネットは、個々のサイトをNDO編成のマルチサイトファブリックに移行する場合にのみ使用してください。移行が完了したら、これらのフラグを無効にできます。

ステップ4 BDの1つ以上の[サブネット (Subnets)]を追加します。

a) [+ サブネットの追加 (+ Add Subnet)] をクリックします。

[サブネットの新規追加 (Add New Subnet)] ウィンドウが開きます。

b) サブネットの[ゲートウェイ IP (Gateway IP)] アドレスと追加するサブネットの[説明 (Description)] を入力します。

c) 必要に応じて、[仮想IPアドレスとして扱う (Treat as virtual IP address)] オプションを有効にします。

このオプションは、BDの[仮想MACアドレス (Virtual MAC Address)] とともに、個々の共通パーベイスンブゲートウェイ設定からNDO統合Multi-Site展開への移行シナリオに使用できます。

d) サブネットの[範囲 (Scope)] を選択します。

これはサブネットのネットワーク可視性です。

- [VRF に対してプライベート (Private to VRF)] : サブネットが L3Out を介して外部ネットワークドメインにアナウンスされないようにします。
- 外部にアドバタイズ (Advertised Externally) : サブネットは L3Out を介して外部ネットワークドメインに向けてアナウンスできます。

e) (任意) [VRF 間で共有 (Shared Between VRFs)] をオンにします。

[VRF 間で共有 (Shared Between VRF)] : サブネットは、同じテナント内で、または共有サービスの一部としてテナントを越えて、複数のコンテキスト (VRF) で共有し、それらにエクスポートすることができます。共有サービスの例は、別のテナントの別のコンテキスト (VRF) に存在する EPG へのルーテッド接続です。これにより、トラフィックはコンテキスト (VRF) 間で双方向に通過できます。共有サービスを提供する EPG は、その EPG の下で (ブリッジドメインの下ではなく) サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF 間で共有する必要があります。

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

f) [デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] オプションはオフのままにします。

このオプションを有効にすると、リーフルルートにプロキシルート (スパインプロキシへのサブネットルート) だけがプログラムされ、SVI は作成されません。つまり、SVI はゲートウェイとして使用できません。

EPG サブネットはルート リークにのみ使用されるため、ゲートウェイとして BD サブネットによって SVI を作成し、EPG で **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]** オプションを有効にすることを勧めます。

- g) (オプション) **[クエリア (Querier)]** オプションを有効にします。
サブネットでの **[IGMP スヌーピング (IGMP Snooping)]** を有効にします。
- h) (オプション) **[プライマリ (Primary)]** オプションを有効にして、サブネットをプライマリとして指定します。
1 つのプライマリ IPv4 サブネットと 1 つのプライマリ IPv6 サブネットが可能です。
- i) **[保存 (Save)]** をクリックします。

ステップ 5 (オプション) **[DHCP ポリシー (DHCP Policy)]** を追加します。

詳細については、[DHCP リレー \(201 ページ\)](#) を参照してください。

ステップ 6 必要に応じて、ブリッジドメインのサイトローカル プロパティを設定します。

[ブリッジドメインのサイトローカルプロパティの設定 \(32 ページ\)](#) で説明されているように、テンプレートレベルの設定に加えて、ブリッジドメインの 1 つ以上のサイトローカルプロパティを定義することもできます。

ブリッジドメインのサイトローカル プロパティの設定

テンプレートでオブジェクトを作成するときにオブジェクトに対して通常設定するテンプレートレベルのプロパティに加えて、テンプレートを割り当てる各サイトに固有の 1 つ以上のプロパティを定義することもできます。

オブジェクトを複数のサイトに展開すると、同じテンプレートレベルの設定がすべてのサイトに展開され、サイトローカルの設定はそれらの特定のサイトにのみ展開されます。

始める前に

次のものがが必要です。

- [ブリッジドメインの設定 \(28 ページ\)](#) の説明に従って、ブリッジドメインを作成し、そのテンプレートレベルのプロパティを設定していること。
- ブリッジドメインを含むテンプレートを 1 つ以上のサイトに割り当てていること。

ステップ 1 ブリッジドメインを含むテンプレートを含むスキーマを開きます。

ステップ 2 左側のサイドバーで、設定する特定のサイトの下のブリッジドメインを含むテンプレートを選択します。

ステップ 3 メインペインで、ブリッジドメインを選択します。

ほとんどのフィールドでは、テンプレートレベルで設定した値が表示されますが、ここでは編集できません。

ステップ 4 [+ L3Out] をクリックして L3Out を追加します。

これは、リモート L3Out から BD サブネットをアドバタイズし、ローカル L3Out に障害が発生した場合でも BD へのインバウンドトラフィックを維持できるようにするために必要です。この場合、サブネットに [外部にアドバタイズ (Advertised Externally)] フラグを設定する必要があります。詳細に関しては、[サイト内 L3Out \(215 ページ\)](#) ユース ケースの例を参照してください。

ステップ 5 [ホストルート (Host Route)] を有効にします。

これにより、ブリッジドメインでホストベースルーティングが有効になります。このノブを有効にすると、ボーダーリーフスイッチは、サブネットとともに個々のエンドポイント (EP) ホストルート (/32 または /128 プレフィックス) もアドバタイズします。ルート情報は、ホストがローカル POD に接続されている場合にのみアドバタイズされます。EP がローカル Pod から離れた、または EP が EP データベースから削除された場合、ルートアドバタイズメントはその時に撤回されます。

ステップ 6 必要に応じて、[SVI MAC アドレス (SVI MAC Address)] を変更します。

仮想 MAC および仮想 IP が Common Pervasive Gateway (CPG) シナリオで有効になっている場合、SVI MAC アドレスはサイトごとに一意である必要があります。このフィールドは、BD のデフォルトルータ MAC を変更する CPG が有効になっていない場合にも使用できます。

アプリケーション プロファイルと EPG の設定

このセクションでは、アプリケーション プロファイルと EPG を設定する方法について説明します。

始める前に

[スキーマとテンプレートの作成 \(24 ページ\)](#) の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

このセクションでは、契約とブリッジドメインが作成されていることも前提としています。

ステップ 1 スキーマを選択し、アプリケーション プロファイルを作成するテンプレートを選択します。

ステップ 2 アプリケーション プロファイルを作成します。

- a) メインペインで、[+ オブジェクトの作成 (+Create Object)] > [アプリケーション プロファイル (Application Profile)] を選択します。

または、[アプリケーション プロファイル (Application Profile)] エリアまでスクロールダウンし、タイトルの上にマウスを移動して、[アプリケーション プロファイルの追加 (Add Application Profile)] をクリックします。

- b) 右側のペインで、アプリケーション プロファイルの [表示名 (Display Name)] を入力します。

競合することなく、異なるテンプレートに同じ名前 of アプリケーション プロファイルを作成できます。ただし、同じサイトおよびテナントに展開する場合は、異なるテンプレートで同じ名前を持つ他のオブジェクト (VRF、BD、EPG など) を作成することはできません。

- c) (任意) [説明 (Description)] を入力します。

ステップ 3 EPG を作成します。

- a) メインペインで[+オブジェクトの作成(Create Object)]>[EPG]を選択し、EPGを作成するアプリケーションプロファイルを選択します。

または、特定の [アプリケーション プロファイル (Application Profile)] エリアまでスクロールダウンし、[EPGs] タイルの上にマウスを移動して、[EPG の追加 (Add EPG)] をクリックします。

- b) 右側のペインで、EPG の [表示名 (Display Name)] を入力します。
- c) (任意) [説明 (Description)] を入力します。

ステップ 4 EPG のコントラクトを追加します。

コントラクトとフィルタの作成については、[コントラクトとフィルタの設定 \(39ページ\)](#) で詳しく説明しています。コントラクトを作成済みの場合：

- a) [+ コントラクト (+ Contract)] をクリックします。
- b) [コントラクトの追加 (Add Contract)] ダイアログで、コントラクトの名前とタイプを入力します。
- c) [保存 (SAVE)] をクリックします。

ステップ 5 [ブリッジ ドメイン (Bridge Domain)] ドロップダウンで、この EPG のブリッジ ドメインを選択します。オンプレミスの EPG を設定する場合は、ブリッジ ドメインに関連付ける必要があります。

ステップ 6 (オプション) [+ サブネット (+ Subnet)] をクリックして、EPG にサブネットを追加します。

たとえば、VRF ルートリークのユースケースとして、ブリッジ ドメイン レベルではなく EPG レベルでサブネットを設定することもできます。

- a) [サブネットの追加 (Add Subnet)] ダイアログで、[ゲートウェイ IP (Gateway IP)] アドレスと追加予定のサブネットの説明を入力します。
- b) [範囲 (Scope)] フィールドで [VRF にプライベート (Private to VRF)] または [外部にアドバタイズ (Advertised Externally)] のどちらかを選択します。
- c) 適切な場合、[VRF 間で共有 (Shared Between VRFs)] チェックボックスをチェックします。
- d) 必要に応じて、[デフォルトの SVI ゲートウェイなしデフォルト (No Default SVI Gateway)] をオンにします。
- e) [OK] をクリックします。

ステップ 7 (オプション) マイクロセグメンテーションを有効にします。

マイクロセグメンテーション EPG (uSeg) を設定する場合は、エンドポイントを EPG に一致させるために 1 つ以上の uSeg 属性を指定する必要があります。

- a) [uSeg EPG] チェックボックスをオンにします。
- b) [+uSeg EPG] をクリックします。
- c) uSeg 属性の [名前 (Name)] と [タイプ (Type)] を入力します。
- d) 選択した属性タイプに基づいて、属性の詳細を指定します。

たとえば、属性タイプとして 1[MAC] を選択した場合は、この EPG でエンドポイントを識別する MAC アドレスを指定します。

e) **[保存 (SAVE)]** をクリックします。

ステップ 8 (オプション) EPG 内分離を有効にします。

デフォルトでは、EPG 内のエンドポイントが自由に相互に通信できます。エンドポイントを互いに分離するには、分離モードを **[強制 (Enforced)]** に設定します。

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

ステップ 9 (オプション) EPG のレイヤ 3 マルチキャストを有効にします。

Layer 3 マルチキャストの詳細については、次を参照してください: [レイヤ 3 マルチキャスト \(265 ページ\)](#)

ステップ 10 (オプション) EPG の優先グループメンバシップを有効にします。

優先グループ機能を使用すると、単一の VRF 内に複数の EPG を含めて、コントラクトを作成しなくても、それらの間の完全な通信を可能にすることができます。EPG 優先グループの詳細については、次を参照してください: [EPG 優先グループ \(211 ページ\)](#)

ステップ 11 必要に応じて、EPG のサイトローカル プロパティを設定します。

[EPG のサイトローカル プロパティの設定 \(35 ページ\)](#) で説明しているように、テンプレート レベルの設定に加えて、EPG の 1 つ以上のサイトローカル プロパティを定義することもできます。

EPG のサイトローカル プロパティの設定

テンプレートでオブジェクトを作成するときにオブジェクトに対して通常設定するテンプレート レベルのプロパティに加えて、テンプレートを割り当てる各サイトに固有の 1 つ以上のプロパティを定義することもできます。

オブジェクトを複数のサイトに展開すると、同じテンプレート レベルの設定がすべてのサイトに展開され、サイトローカルの設定はそれらの特定のサイトにのみ展開されます。

始める前に

次のものが必要です。

- [アプリケーション プロファイルと EPG の設定 \(33 ページ\)](#) の説明に従って作成されたアプリケーション プロファイルと EPG。テンプレート レベルでプロパティが設定されていることも必要です。
- ブリッジ ドメインを含むテンプレートを 1 つ以上のサイトに割り当てていること。

ステップ 1 EPG でテンプレートを含むスキーマを開きます。

ステップ 2 左側のサイドバーで、設定する特定のサイトの下の EPG を含むテンプレートを選択します。

ステップ3 メインペインで、EPG を選択します。

ほとんどのフィールドでは、テンプレート レベルで設定した値が表示されますが、ここでは編集できません。

ステップ4 EPG に1つ以上のサブネットを追加します。

a) **[+ サブネットの追加 (+ Add Subnet)]** をクリックします。

[サブネットの新規追加 (Add New Subnet)] ウィンドウが開きます。

b) サブネットの **ゲートウェイ IP** アドレスと追加するサブネットの説明を入力します。

c) サブネットの **[範囲 (Scope)]** を選択します。

これはサブネットのネットワーク可視性です。

- **[VRF に対してプライベート (Private to VRF)]** : サブネットが **L3Out** を介して外部ネットワーク ドメインにアナウンスされないようにします。

- **外部にアドバタイズ (Advertised Externally)** : サブネットは **L3Out** を介して外部ネットワークドメインに向けてアナウンスできます。

d) (任意) **[VRF 間で共有 (Shared Between VRFs)]** をオンにします。

[VRF 間で共有 (Shared Between VRF)] : サブネットは、同じテナント内で、または共有サービスの一部としてテナントを越えて、複数のコンテキスト (VRF) で共有し、それらにエクスポートすることができます。共有サービスの例は、別のテナントの別のコンテキスト (VRF) に存在する EPG へのルーテッド接続です。これにより、トラフィックはコンテキスト (VRF) 間で双方向に通過できます。共有サービスを提供する EPG は (EPG ではなく) **BD** でサブネットを設定する必要があり、そのスコープは外部にアドバタイズされ、VRF 間で共有されるように設定する必要があります。

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

e) (オプション) **[デフォルトの SVI ゲートウェイなし (No Default SVI Gateway)]** を有効にします。

このオプションを有効にすると、リーフルートにプロキシルート (スパインプロキシへのサブネットルート) だけがプログラムされ、SVI は作成されません。つまり、SVI はゲートウェイとして使用できません。

EPG サブネットではこのオプションを有効にすることをお勧めします。このオプションは、ルート リークにのみ使用し、**BD** サブネットではこのオプションを無効のままにして、**SVI** をゲートウェイとして使用できるようにします。

f) **[保存 (Save)]** をクリックします。

ステップ5 1つ以上のスタティックポートを追加します。

a) **[+ スタティック ポートの追加 (+Static Port)]** をクリックします。

b) **[パスタイプ (Path Type)]** ドロップダウンから、ポートのタイプを選択します。

c) 物理インターフェイスを構成する場合は、**[ポッド (Pod)]** を選択します。

d) 単一のポートを構成するか、ポートの範囲を構成するかを選択します。

インターフェイス設定については、単一のリーフとパスを入力するか、リーフの範囲（例：120 - 125 およびパス）を入力して（例：1/17-20）するオプションがあります。また、リーフの範囲を入力して 1 つの単一のパスに関連付けるか、1 つの単一のリーフのパスの範囲を入力するオプションもあります。

ただし、構成後も UI には個別のポートとして表示され、今後の更新では個別の変更が必要になります。

- e) [ポート カプセル化 VLAN (Port Encap VLAN)] を選択します。

EPG のドメインでポート カプセル化を手動で設定する場合、VLAN ID はダイナミック VLAN プール内のスタティック VLAN ブロックに属している必要があります。

EPG でテンプレート レベルでのマイクロセグメンテーションが有効になっている場合、**プライマリ MICRO-SEG VLAN** が設定されると、ポート カプセル化 VLAN はプライマリ VLAN の独立した**セカンダリ VLAN** として設定されます。トラフィックはセカンダリ VLAN を使用してホストからリーフに送信され、リーフからホストへのリターン トラフィックはプライマリ VLAN を使用して送信されます。

- f) （任意）**プライマリ MICRO-SEG VLAN (Primary MICRO-SEG VLAN)** を選択します。

マイクロセグメンテーションの VLAN 識別子

- g) （オプション）**[展開の即時性 (Deployment Immediacy)]** を選択します。

ポリシーがリーフ ノードにダウンロードされたときに、ポリシーがハードウェア ポリシー CAM にプッシュされるタイミングは、展開の即時性によって指定できます。

- [即時 (Immediate)] : リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
- [オンデマンド (On Demand)] : 最初のパケットがデータ パス経路で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

- h) （オプション）**[モード (Mode)]** を選択します。

パスのスタティック アソシエーションのモードを選択します。EPG のタグ付けとは、EPG で次のようにスタティック パスを設定することです。

- [トランク (Trunk)] : これはデフォルトの展開モードです。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、このモードを選択します。
- [アクセス (802.1P) (Access (802.1P))] : ホストからのトラフィックが 802.1P タグでタグ付けされている場合、このモードを選択します。アクセス ポートにネイティブ 802.1p モードの EPG を 1 つ設定すると、そのパケットはタグなしの状態ですべてのポートを退出します。ネイティブ 802.1p モードの EPG を 1 つと、VLAN タグが付いた複数の EPG をアクセス ポートに設定すると、ネイティブ 802.1p モードで設定された EPG については、そのアクセス ポートを退出するすべてのパケットに VLAN 0 がタグ付けされ、退出する他のすべての EPG パケットにはそれぞれの VLAN タグが付けられます。1 つのアクセス ポートにつき、ネイティブ 802.1p EPG は 1 つだけ許可されることに注意してください。

- [アクセス (タグなし) (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 (VLAN ID なし)、このモードを選択します。ある EPG が使用するすべてのポートについて、この EPG にタグ付けしないようリーフ スイッチを設定すると、パケットはタグなしの状態ですイッチから送出されます。EPG をタグなしとして展開する際は、その EPG を同じスイッチの他のポート上にタグ付きとして展開することは避ける必要があることに注意してください。

ステップ 6 1 つ以上のスタティック リーフノードを追加します。

- [+ スタティック リーフの追加 (+Static Leaf)] をクリックします。
- [リーフ (Leaf)] ドロップダウンから、追加するリーフ ノードを選択します。
- (任意) [VLAN] フィールドに、タグ付きトラフィックの VLAN ID を入力します。

ステップ 7 1 つ以上のドメイン ノードを追加します。

- [+ ドメイン (+Domain)] をクリックします。
- [ドメイン関連付けタイプ (Domain Association Type)] を選択します。

これは、追加するドメインのタイプです。

- VMM
 - Fibre Channel
 - L2 外部
 - L3 外部
 - 物理
- [ドメイン プロファイル (Domain Profile)] の名前を選択します。
 - [展開の即時性 (Deployment Immediacy)] を選択します。

導入の即時性で、ポリシーがプッシュされるタイミングを指定できます。

- [即時 (Immediate)] : リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
 - [オン デマンド (On Demand)] : 最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。
- [解決の即時性 (Resolution Immediacy)] を選択します。

ポリシーをすぐに解決するか、必要に応じて解決するかを指定します。次のオプションがあります。

- [即時 (Immediate)] : ハイパーバイザが VMware vSphere Distributed Switch (VDS) に接続されると、EPG ポリシーがリーフ スイッチ ノードにプッシュされるように指定します。LLDP または OpFlex 権限は、ハイパーバイザ/リーフ ノード接続を解決するために使用されます。
- [オン デマンド (On Demand)] : ハイパーバイザが VDS に接続され、VM がポート グループ (EPG) に配置されている場合にのみ、EPG ポリシーがリーフ スイッチ ノードにプッシュされるように指定します。

- [事前プロビジョニング (Pre-provision)] : ハイパーバイザが VDS に接続される前でも、EPG ポリシーがリーフスイッチ ノードにプッシュされるように指定します。スイッチ上の設定がダウンロードにより事前プロビジョニングされます。

コントラクトとフィルタの設定

ここでは、コントラクトとフィルタを設定し、フィルタをコントラクトに割り当てる方法について説明します。フィルタはアクセス コントロール リスト (ACL) に似ています。これは EPG に関連付けられた契約を通して、トラフィックをフィルタします。

ステップ 1 スキーマを選択し、コントラクトとフィルタを作成するテンプレートを選択します。

コントラクトは、適用するオブジェクト (EPG および外部 EPG) と同じテンプレートでも異なるテンプレートでも作成できます。コントラクトを使用するオブジェクトが異なるサイトに展開されている場合は、複数のサイトに関連付けられたテンプレートでコントラクトを定義することをお勧めします。ただし、これは必須ではありません。コントラクトとフィルタが Site1 のローカル オブジェクトとしてのみ定義されている場合でも、Site2 のローカル EPG または外部 EPG がそのコントラクトを使用または提供する必要がある場合、NDO はそれらのオブジェクトをリモート Site2 に作成します。

ステップ 2 フィルタを作成します。

- a) メインペインで、[+ オブジェクトの作成 (+Create Object)] > [フィルタ (Filter)] を選択します。

または、[フィルタ (Filters)] エリアまでスクロール ダウンし、タイルの上にマウスを移動して、[フィルタの追加 (Add Filter)] をクリックします。

- b) 右側のペインで、フィルタの [表示名 (Display Name)] を入力します。
c) (任意) [説明 (Description)] を入力します。

ステップ 3 フィルタ エントリを作成します。

- a) 右側のペインで、[+ エントリ (+ Entry)] をクリックします。

フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。次の手順の説明に従って、1 つ以上のオプションを指定できます。

- b) フィルタの [名前 (Name)] を指定します。
c) [イーサー タイプ (Ether Type)] を選択します。

たとえば [ip] です。

- d) [IP プロトコル (IP Protocol)] を選択します。

たとえば [icmp] です。

- e) [宛先ポート範囲の開始 (Destination Port Range From)] と [宛先ポート範囲の終了 (Destination Port Range To)] を選択します。

宛先ポート範囲の開始と終了です。開始フィールドと終了フィールドに同じ値を指定すれば、単一のポートの指定になります。または、0 から 65535 の範囲内で、ポートの範囲を定義することもできます。また、特定のポート番号 (http など) の代わりに、いずれかのサーバタイプを指定することもできます。

- f) **[フラグメントのみの一致 (Match only fragment)]** オプションを有効にします。

有効の場合、オフセットが 0 より大きいすべての IP フラグメント (最初のフラグメントを除くすべての IP フラグメント) にこのルールが適用されます。無効の場合、TCP/UDP ポート情報は最初のフラグメントでしかチェックできないため、オフセットが 0 より大きい IP フラグメントにルールは適用されません。

- g) **[ステートフル (Stateful)]** オプションを有効にします。

このオプションを有効にする場合には、プロバイダーからコンシューマに戻るすべてのトラフィックは、常にパケットに ACK ビットが設定されている必要があります。そうでないと、パケットはドロップされます。

- h) **[ARP フラグ (ARP flag)]** : (Address Resolution Protocol) を指定します。

ARPフラグは、ARP の特定のフィルタを作成するときに使用され、ARP 要求または ARP 応答を指定できます。

- i) **[送信元ポート範囲の開始 (Source Port Range From)]** と **[送信元ポート範囲の終了 (Source Port Range To)]** を指定します。

送信元ポート範囲の開始と終了です。開始フィールドと終了フィールドに同じ値を指定すれば、単一のポートの指定になります。または、0 から 65535 の範囲内で、ポートの範囲を定義することもできます。また、特定のポート番号 (http など) の代わりに、いずれかのサーバタイプを指定することもできます。

- j) **[TCP セッションルール (TCP session rules)]** を指定します。

TCPセッションルールは、TCPトラフィックのフィルタを作成するときに使用され、ステートフルACLの動作を設定できます。

- k) **[保存 (Save)]** をクリックしてフィルタを保存します。

- l) このフィルタの追加のフィルタ エントリを作成するには、この手順を繰り返します。

フィルタごとに複数のフィルタ エントリを作成して割り当てることができます。

ステップ 4 コントラクトの作成

- a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[コントラクト (Contract)]** を選択します。

または、**[コントラクト (Contract)]** エリアまでスクロールダウンし、タイルの上にマウスを移動して、**[コントラクトの追加 (Add Contract)]** をクリックします。

- b) 右側のペインで、コントラクトの**表示名**を指定します。

- c) (任意) **[説明 (Description)]** を入力します。

- d) コントラクトの適切な**[範囲 (Scope)]** を選択します。

コントラクトの範囲によって、コントラクトのアクセシビリティが制限されます。契約は、プロバイダ EPG の範囲外のコンシューマ EPG には適用されません。

- アプリケーションプロファイル
- vrf
- テナント
- global

- e) コンシューマからプロバイダーへの方向とプロバイダーからコンシューマへの方向の両方に同じフィルタを適用する場合は、**[両方向に適用 (Apply both directions)]** ノブを切り替えます。

このオプションを有効にした場合は、フィルタを 1 回だけ指定することが必要となり、両方向のトラフィックに適用されます。このオプションを無効のままにした場合は、各方向に1つずつ、2セットのフィルタ チェーンを指定する必要があります。

(注) **[両方向に適用 (Apply both directions)]** を有効にしてコントラクトを作成および展開する場合は、単にオプションを無効にしたり、変更を適用して再展開したりすることはできません。すでに展開されているコントラクトでこのオプションを無効にするには、コントラクトを削除し、テンプレートを展開してから、オプションを無効にしてコントラクトを再作成し、ファブリックの設定を正しく変更する必要があります。

- f) (オプション) **[サービス グラフ (Service Graph)]** ドロップダウンから、このコントラクトのサービスグラフを選択します。
- g) (オプション) **[QoS レベル (QoS Level)]** ドロップダウンから、このコントラクトの値を選択します。

この値には、このコントラクトを使用してトラフィックに割り当てられる ACI QoS レベルを指定します。詳細については、[IPN 全体での QoS の保持 \(279 ページ\)](#) を参照してください。

これを [未指定 (Unspecified)] のままにすると、デフォルトの QoS レベル3 がトラフィックに適用されます。

ステップ 5 コントラクトにフィルタを割り当てる

- a) 右側のペインで、**[フィルタ チェーン (Filter Chain)]** 領域までスクロールし、**[+ フィルタ (+ Filter)]** をクリックしてフィルタをコントラクトに追加します。
- b) 開いた**[フィルタ チェーンの追加]** ウィンドウで、**[名前 (Name)]** ドロップダウンメニューから前の手順で追加したフィルタを選択します。
- c) フィルタの**[アクション (Action)]** を選択します。

フィルタを追加するときに、フィルタ条件に一致するトラフィックを許可するか拒否するかを選択できます。[拒否 (deny)] フィルタの場合、[デフォルト (default)]、[低 (low)]、[中 (medium)]、または [高 (high)] の 4 段階のレベルのいずれかにフィルタの優先順位を設定できます。[許可 (permit)] フィルタは常にデフォルトの優先順位を持ちます。ACI コントラクトとフィルタの詳細については、『[Cisco ACI Contract Guide](#)』を参照してください。

- d) **[保存 (Save)]** をクリックして、フィルタをコントラクトに追加します。
- e) コントラクトで **[両方向に適用 (Apply both directions)]** オプションを無効にした場合は、他のフィルタチェーンに対してこの手順を繰り返します。

f) (オプション) 複数のフィルタを作成して各コントラクトに割り当てることができます。

同じコントラクトに追加のフィルタを作成する場合：

- ステップ 2 とステップ 3 を繰り返して、フィルタ エントリとともに別のフィルタを作成します。
- この手順を繰り返して、このコントラクトに新しいフィルタを割り当てます。

オンプレミス外部接続の設定

Cisco ACI では、境界リーフ スイッチを介してオンプレミス ACI ファブリックの外部のネットワークへの接続を確立できます。この接続は、セキュリティとルートマップを定義するために必要な設定オプションを提供する L3Out と外部 EPG の 2 つの構造を使用して定義されます。

このセクションでは、Nexus Dashboard Orchestrator GUI を使用して L3Out と外部 EPG を追加する方法について説明します。次に、Orchestrator で、テンプレートを展開する APIC サイトにおいてオブジェクトを作成します。Orchestrator から L3Out を作成する場合、APIC では L3Out コンテナ オブジェクトのみが作成されることに注意してください。この場合も、サイトの APIC で、完全な L3Out の構成 (ノード、インターフェイス、ルーティングプロトコルなど) を直接実行する必要があります。

ほとんどの場合、L3Out は APIC レベルで直接作成され、その後、Orchestrator で作成した外部 EPG に関連付けられます。L3Out を Orchestrator から作成した VRF に直接関連付ける場合には、ここで両方を作成すると便利です。

始める前に

- [スキーマとテンプレートの作成 \(24 ページ\)](#) の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。
- [VRF の設定 \(27 ページ\)](#) の説明に従って、L3Out の VRF を作成する必要があります。

ステップ 1 編集するスキーマとテンプレートに移動します。

ステップ 2 L3Out を作成します。

- [スキーマ編集 (schema edit)] ビューで、**[L3Out]** エリアまで下にスクロールし、+ をクリックして新しい L3Out を追加します。
- 右側のプロパティ ペインで、L3Out の [表示名 (Display Name)] を入力します。
- [仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した VRF を選択します。

ステップ 3 外部 EPG を作成します。

- [スキーマ編集 (Schema edit)] ビューで、**[外部 EPG (External EPG)]** エリアまでスクロールし、[+ をクリックして、新しい外部 EPG をクリックします。
- 右側のプロパティ ペインで、サイトタイプとして **[オンプレミス (On-Prem)]** を選択します。

ステップ 4 外部 EPG の基本的なプロパティを設定します。

- a) 右側のプロパティ サイドバーで、外部 EPG の表示名を指定します。
- b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した VRF を選択します。

これは、L3Out に関連付けた VRF と同じである必要があります。

- c) **[+ コントラクト (+ Contract)]** をクリックして、外部 EPG が他の EPG と通信するためのコントラクトを追加します。

すでにコントラクトを作成している場合は、ここでコントラクトを割り当てることができます。それ以外の場合、後ほど作成する予定のコントラクトは、この画面に戻って割り当てることができます。

コントラクトを割り当てる場合：

- 契約をプロバイダとしての外部 EPG に関連付ける場合には、外部 EPG に関連付けられているテナントから、コントラクトだけを選択します。その他のテナントからは、コントラクトを選択しないでください。
- コントラクトをコンシューマとしての外部 EPG に関連付ける場合には、利用可能な任意のコントラクトから選択できます。

ステップ 5 オンプレミス ファブリックの外部 EPG を設定する場合は、**[サイト タイプ (Site Type)]** を [オンプレミス (on-prem)] に設定し、外部 EPG のオンプレミス プロパティを設定します。

- a) **[L3Out]** ドロップダウン メニューから、前の手順で作成した L3Out を選択します。

(注) テンプレート レベルまたはサイトローカル レベルで L3Out を選択できます。サイトローカル レベルで外部 EPG の L3Out を設定することを推奨します。これを行うには、割り当てられているサイトの下の左側のサイドバーでテンプレートを選択します。次に、外部 EPG を選択し、L3Out をそれに関連付けます。

- b) **[+ サブネット (+Subnet)]** をクリックしてサブネットを追加します。

これは、分類サブネットまたはルート制御に使用されるサブネットです。

- c) **[サブネット追加 (Add Subnet)]** ウィンドウで、サブネットのプレフィックスを入力します。
- d) 必要な **[ルート制御 (Route Control)]** オプションを選択します。

次のいずれかのオプションを 1 つ、または複数選択できます。

- **[エクスポート ルート制御 (Export Route Control)]** より、ルートマップを有効にして、指定されたサブネットプレフィックスに一致する外部プレフィックスを L3Out からアドバタイズできるようにします。これらは、中継ルーティングの使用例で他の L3Out から学習したプレフィックスです。

0.0.0.0/0 サブネットを追加し、エクスポート ルート制御オプションを有効にすると、**[集約エクスポート (Aggregate Export)]** オプションが使用可能になります。これにより、他の L3Out から学習したすべての外部プレフィックスをアドバタイズできます。このオプションを無効のままにすると、他の L3Out から学習したデフォルト ルートのみがこの L3Out からアドバタイズされます。

- **[インポート ルート制御 (Import Route Control)]** は、入力ルートマップを設定して、L3Out からファブリックにインポートするプレフィックスを制御します。**[インポート ルート制御 (Import Route Control)]** は、L3Out でルーティング プロトコルとして BGP を使用する場合にのみ使用できます。

0.0.0.0/0 サブネットを追加し、インポートルート制御オプションを有効にすると、**[集約インポート (Aggregate Import)]** オプションが使用可能になります。これは、入力ルートを除き、エクスポートルート制御の場合と同様に機能します。

- **[共有ルート制御 (Shared Route Control)]** は、共有 L3Out の使用例で使用され、外部ルータから学習したプレフィックスを、この L3Out を使用する他の VRF にアドバタイズできます。

共有ルート制御オプションを有効にすると、**[集約教諭ルート]** オプションが使用可能になります。繰り返しますが、これは前の2つの集約ルートオプションに似ています。ただし、0.0.0.0/0 以外のサブネットで使用できます。

- e) **[外部 EPG 分類 (External EPG Classification)]** オプションを選択します。

外部エンティティをこの特定の外部 EPG にマッピングできるようにするには、設定されたサブネットの **[外部 EPG 向けの外部サブネット (External Subnets for External EPG)]** オプションをオンにする必要があります。これにより、これらの外部ネットワークとファブリック内で定義された EPG に属するエンドポイント間にセキュリティポリシー（コントラクト）を適用できます。0.0.0.0/0 プレフィックスに対してこのフラグを有効にすると、すべての外部宛先がこの外部 EPG の一部と見なされます。

このオプションを有効にすると、**[共有セキュリティインポート (Shared Security Import)]** オプションが使用可能になり、サブネットから VRF 間（共有サービス）での使用例のエンドポイントへのアクセスが可能になります。

これらの両方のオプションでは、アクセスは引き続きコントラクトルールに従います。

ステップ 6 クラウドファブリックの外部 EPG を設定する場合は、**[サイト タイプ (Site Type)]** を [クラウド (cloud)] に設定し、外部 EPG のクラウドプロパティを設定します。

- [アプリケーション プロファイル (Application Profile)]** ドロップダウンから、アプリケーションプロファイルを選択します。
- [+ セレクタの追加 (+ Add Selector)]** をクリックして、EPG のクラウドエンドポイントセレクタを追加します。

ステップ 7 （オプション）優先グループにこの外部 EPG を含める場合は、**[優先グループに含める (Include in preferred group)]** チェックボックスをオンにします。

EPG 優先グループの詳細については、[EPG 優先グループ \(211 ページ\)](#) を参照してください。

スキーマの表示

1 つまたは複数のスキーマを作成すると、**[ダッシュボード (Dashboard)]** および **[スキーマ (Schemas)]** ページの両方に表示されます。

これら2つのページで使用可能な機能を使用して、展開時の使用率とスキーマの状態をモニタできます。Nexus Dashboard Orchestrator GUI を使用して、実装されたスキーマ ポリシーの特定の領域にアクセスして編集することもできます。

テンプレートオブジェクトの一括更新

一括更新機能を使用すると、テンプレート内の同じタイプの複数の異なるオブジェクトの複数のプロパティを一度に更新できます。たとえば、各オブジェクトを個別に変更する代わりに、同時に2つ以上の EPG にインフラ EPG 分離を適用できます。このワークフローを使用する場合、選択したすべてのオブジェクトは同じタイプである必要があります。たとえば、EPG と BD を同時に更新することはできません。

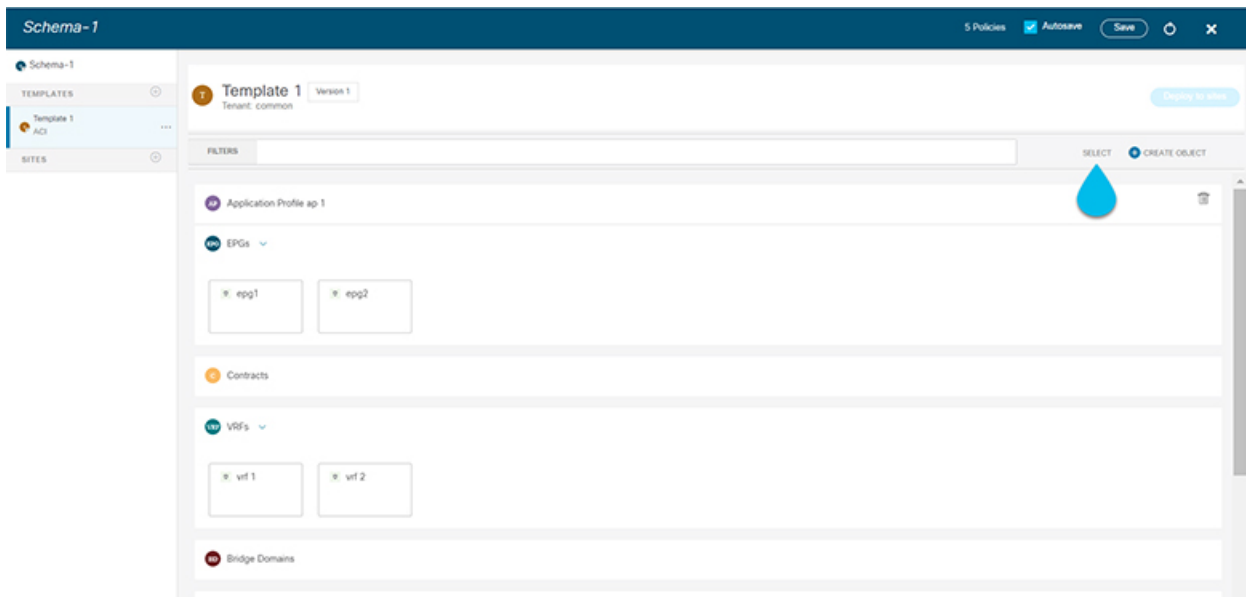
選択したオブジェクトにすでに別のプロパティ値が構成されている場合、更新により、それらのプロパティが指定した値で上書きされます。この機能により、オンプレミスのテンプレートレベルのオブジェクトプロパティを更新できます。サイトローカルプロパティとクラウドプロパティの更新はサポートされていません。



(注) この機能は、Cisco APIC および Cisco DCNM ファブリックでのみサポートされています。Cisco Cloud APIC サイトではサポートされていません。

ステップ 1 更新するオブジェクトが含まれているスキーマに移行します。

ステップ 2 右上のペインから、「選択」を選択します。同じタイプのオブジェクトを複数選択できます。

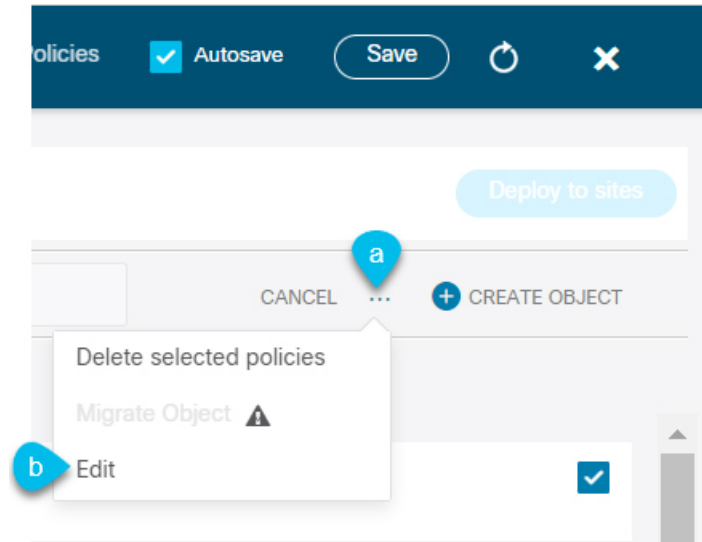


ステップ 3 更新するすべてのオブジェクトを選択した後。

a) キャンセル オプションの横にある [...] を選択します。

b) ドロップダウンから「編集」を選択します。

異なるタイプのオブジェクトを選択した場合、ドロップダウンに [編集 (Edit)] オプションは表示されません。

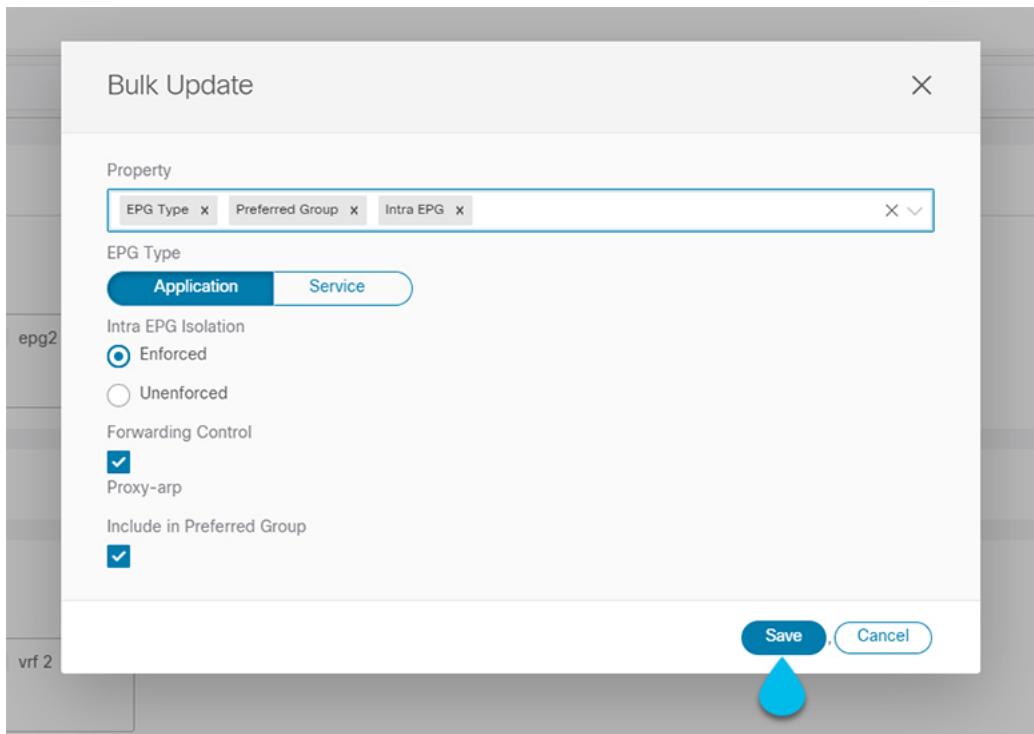


ステップ 4 [編集 (Edit)] を選択すると、ポップアップが表示されます。選択したオブジェクトのプロパティのサブセットが表示されます。

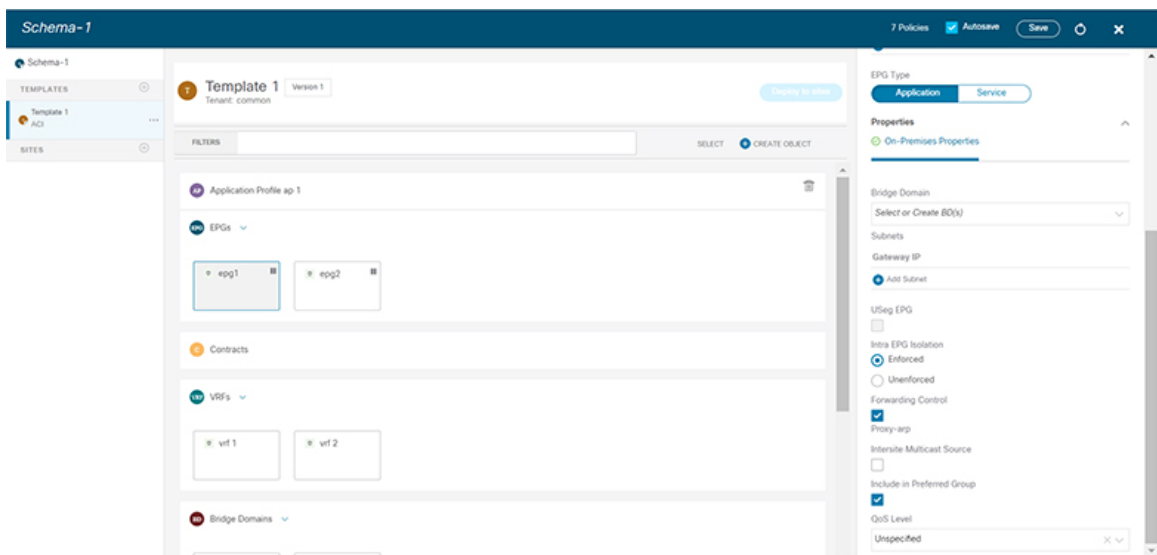
選択したオブジェクトのタイプに基づいて、次のプロパティを更新できます。

1. **[EPG]**: ブリッジドメイン、コントラクト、EPG タイプ、インフラ EPG、優先グループ。
2. **[コントラクト (Contracts)]**: 範囲、フィルターチェーン、QOS レベル。
3. **[VRF]**: IP データプレーン学習。
4. **[ブリッジドメイン (Bridge Domain)]**: 仮想ルーティングとフォワーワーディング、L2 ストレッチ、L2 不明なユニキャスト、不明なマルチキャスト フラッドディング、IPv6 不明なマルチキャスト フラッドディング、複数宛先フラッドディング、DHCP ポリシー、ユニキャスト ルーティング。
5. **[外部 EPG (External EPG)]**: コントラクト、外部 EPG タイプ、優先グループ。

ステップ 5 すべてのフィールドを選択したら、更新します。[保存 (Save)] を選択すると、先ほど行った更新が実装されます。



ステップ6 更新を保存すると、行った変更を確認できます。



サイトへのテンプレートの割り当て

ここでは、サイトにテンプレートを割り当てる方法について説明します。

始める前に

このドキュメントの前のセクションで説明したように、作成されたサイトには、展開するスキーマ、テンプレート、およびオブジェクトが必要です。

ステップ 1 展開する 1 つ以上のテンプレートを含むスキーマに移動します。

ステップ 2 左側のサイドバーで、サイトに割り当てるテンプレートを選択します。

ステップ 3 テンプレートの名前の横にある **[アクション (Actions)]** メニュー (...) をクリックし、**[サイトの追加 (Add Sites)]** を選択します。

[<template-name> へのサイトの追加] ウィンドウが開きます。

ステップ 4 **[サイトの追加 (Add Sites)]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

選択したテンプレートのタイプとサイト間のサイト間接続によっては、一部のサイトを割り当てに使用できない場合があることに注意してください。

- クラウド ローカルテンプレートを割り当てる場合は、単一のクラウドサイトにのみ割り当てることができます。
- テンプレートを複数のサイトに割り当てる場合、BGP-EVPN プロトコルを使用して、それらのサイト間のサイト間接続を確立する必要があります。パーシャルメッシュ接続があるサイトを選択した場合、サイト間接続がないサイト、または BGP-IPv4 を使用してサイト間接続が確立されているサイトはグレー表示され、割り当てに使用できません。

ステップ 5 **[保存 (Save)]** をクリックします。

一度に 1 つのテンプレートを展開するため、展開できるようにするには、少なくとも 1 つのサイトにテンプレートを関連付ける必要があります。

テンプレートのバージョンニング

テンプレートが保存されるたびに、新しいバージョンのテンプレートが作成されます。NDO UI 内から、テンプレートのすべての設定変更の履歴を、変更者と変更日時に関する情報とともに表示できます。以前のバージョンを現在のバージョンと比較することもできます。

新しいバージョンはスキーマ レベルではなくテンプレート レベルで作成されるため、各テンプレートを個別に設定、比較、ロールバックできます。

テンプレートバージョンは、次のルールに従って作成および管理されます。

- すべてのテンプレートバージョンは、Deployed または Intermediate のいずれかです。

Deployed — サイトに展開されたテンプレートのバージョン。

Intermediate—変更および保存されたが、サイトに展開されていないテンプレートのバージョン。

- テンプレートごとに最大 20 の Deployed バージョンと 20 の Intermediate バージョンをいつでも保存できます。
- 20 バージョンの制限を超える新しい Intermediate バージョンが作成されると、最も古い既存の Intermediate バージョンが削除されます。
- テンプレートが展開され、新しい Deployed バージョンが作成されると、すべての Intermediate バージョンが削除されます。新しい Deployed バージョンが 20 バージョン制限を超えると、最も古い既存の Deployed バージョンが削除されます。
- バージョンに Golden のタグを付けても、保存されているテンプレートバージョンの数には影響しません。
- テンプレートごとに無制限のバージョンをサポートしていた以前のリリースから最初にアップグレードする場合、既存のすべてのバージョンはそのまま残ります。

テンプレートが変更されて保存または展開されると、20 Deployed および 20 Intermediate スケールを超えるバージョンは、上記のルールに従って削除されます。

タギング テンプレート

任意の時点で、テンプレートの現在のバージョンに「ゴールデン」のタグを付けることができます。たとえば、完全に検証された設定で確認、承認、および展開されたバージョンを示すために、今後の参照用に選択できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)] ビューで、確認するテンプレートを選択します。

ステップ 5 テンプレートのアクション (...) メニューから、[ゴールデンとして設定 (Set as Golden)] を選択します。

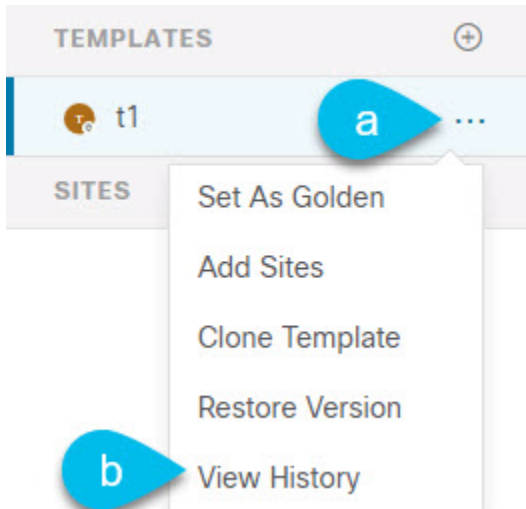
テンプレートがすでにタグ付けされている場合、オプションは [ゴールデンの削除 (Remove Golden)] に変更され、現在のバージョンからタグを削除できます。

タグ付けされたバージョンは、テンプレートのバージョン履歴画面でスターアイコンで示されます。

履歴の表示と以前のバージョンの比較

ここでは、テンプレートの以前のバージョンを表示し、現在のバージョンと比較する方法について説明します。

- ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)]>[スキーマ (Schemas)] を選択します。
- ステップ3 表示するテンプレートを含むスキーマをクリックします。
- ステップ4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。
- ステップ5 テンプレートのアクション (...) メニューから、[履歴の表示 (View History)] を選択します。



- ステップ6 [バージョン履歴 (Version History)] ウィンドウで、適切な選択を行います。

The screenshot shows the 'Version History' window with the following details:

- General Information:** Schema versioning, Template t1, Tenant mso-tenant1.
- Versions:** A timeline showing versions 1, 2, 3, and 4. Version 2 is selected (blue circle), and Version 4 is current (purple circle). Checkboxes for 'Golden Versions' (a) and 'Deployed Versions' (b) are checked.
- Version 2 (Selected):** 1 policy | 0 sites. JSON snippet:


```
1. {
2.   "siteDelta": {},
3. }
4. "anps": [],
5. "bds": [],
34. }
```
- Version 4 (Current):** 2 policies | 1 sites. JSON snippet:


```
1. {
2.   "siteDelta": {
3.     "ø": {
4.       "anps": [],
5.       "bds": [],
6.       "contracts": [],
7.       "externalEggs": [],
8.       "intersitel3outs": [],
9.       "networks": [],
10.      "serviceGraphs": [],
11.      "siteId": "61042fa61a7b8c0a62a1a0c4",
12.      "templateName": "t1",
13.      "vrfs": []
14.    }
15.  },
16.  "template": {
17.    "anps": [],
18.    "bds": [
19.      {
20.        "arpFlood": true,
21.        "bdRef":
22.        "/schemas/610450571f0000a5030540af/templates/t1/bds/bd1",
23.        "dhcpLabels": [],
24.        "displayName": "bd1",
25.        "intersiteBumTrafficAllow": true,
26.        "l3Stretch": true

```

- a) **[ゴールデンバージョン (Golden Versions)]** チェックボックスをオンにして、以前のバージョンのリストをフィルタリングし、Golden としてマークされていたこのテンプレートのバージョンのみを表示します。

「Golden」としてのテンプレートのタグ付けについては、[タギングテンプレート \(49 ページ\)](#) を参照してください。

- b) 以前のバージョンのリストをフィルタリングして、サイトに展開されていたこのテンプレートのバージョンのみを表示するには、**[展開済みバージョン (Deployed Versions)]** チェックボックスをオンにします。

新しいテンプレートバージョンは、テンプレートが変更され、スキーマが保存されるたびに作成されます。ある時点でサイトに実際に展開されたテンプレートのバージョンのみを表示するように選択できます。

- c) 特定のバージョンをクリックして、現在のバージョンと比較します。

選択したバージョンは、常にテンプレートの現在のバージョンと比較されます。[**ゴールデンバージョン (Golden Versions)**] または [**導入済みバージョン (Deployed Versions)**] フィルタを使用してリストをフィルタリングした場合でも、導入済みまたはゴールデンとしてタグ付けされていない場合でも、現在のバージョンが常に表示されます。

- d) [**編集 (Edit)**] アイコンの上にマウスを置くと、バージョンの作成者と作成日時に関する情報が表示されます。

ステップ 7 [**OK**] をクリックして、バージョン履歴ウィンドウを閉じます。

以前の製品バージョンへの復元

ここでは、以前のバージョンのテンプレートを復元する方法について説明します。テンプレートを元に戻す場合、次のルールが適用されます。

- ターゲットバージョンが存在しないオブジェクトを参照している場合、復元操作は許可されません。
- ターゲットバージョンが NDO で管理されなくなったサイトを参照している場合、復元操作は許可されません。
- 現在のバージョンが、ターゲットバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されません。
テンプレートを元に戻す前に、まずそれらのサイトから現在のバージョンを展開解除する必要があります。
- ターゲットバージョンが、現在のバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[**アプリケーション管理 (Application Management)**] > [**スキーマ (Schemas)**] を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)] ビューで、確認するテンプレートを選択します。

ステップ 5 [**アクション (Actions)**] ([...]) メニューから、[**ロールバック (Rollback)**] を選択します。

ステップ 6 [**ロールバック (Rollback)**] ウィンドウで、復元する以前のバージョンのいずれかを選択します。

[**ゴールデンバージョン (Golden Versions)**] チェックボックスと [**展開済みバージョン (Deployed Versions)**] チェックボックスを使用して、バージョンのリストをフィルタリングできます。

バージョンを選択すると、そのバージョンのテンプレート設定をテンプレートの現在のバージョンと比較できます。

ステップ 7 [**復元 (Restore)**] をクリックして、選択したバージョンを復元します。

以前のバージョンを復元すると、前の手順で選択したバージョンと同じ設定の新しいバージョンのテンプレートが作成されます。

たとえば、最新のテンプレートバージョンが 3 で、バージョン 2 を復元すると、バージョン 4 が作成されます。バージョン 2 の設定と同じだからです。復元を確認するには、テンプレートのバージョン履歴を参照し、現在の最新バージョンと復元時に選択したバージョンを比較します。

テンプレートのレビューと承認（変更管理）が無効になっており、アカウントにテンプレートを展開するための適切な権限がある場合は、復元したバージョンを展開できます。

ただし、変更制御が有効になっている場合は、次のようになります。

- 以前に展開したバージョンに戻し、アカウントにテンプレートを展開するための正しい権限がある場合は、すぐにテンプレートを展開できます。
- 以前に展開されていなかったバージョンに戻す場合、またはアカウントにテンプレートを展開するための適切な権限がない場合は、復元されたバージョンを展開する前にテンプレートの承認を要求する必要があります。

レビューと承認プロセスに関する追加情報については、[テンプレートのレビューと承認（53 ページ）](#) セクションを参照してください。

テンプレートのレビューと承認

リリース 3.4(1) では、テンプレートのレビューと承認（変更管理）のワークフローのサポートが追加されます。これにより、テンプレートの設計者、レビュー担当者、承認者、およびテンプレートの導入者に指定されたロールを設定し、また、導入した設定が検証プロセスを確実にパスできるようにします。

テンプレート設計者は、NDO UI 内から、作成したテンプレートのレビューを要求できます。その後、レビュー担当者は、テンプレートのすべての設定変更の履歴と、誰がいつ変更したかに関する情報を表示できます。この時点で、テンプレートの現在のバージョンを承認または拒否できます。テンプレート設定が拒否された場合、テンプレート設計者は必要な変更を行い、レビューを再要求できます。テンプレートが承認されると、展開担当者のロールを持つユーザがサイトに展開できます。最後の点として、導入者自身が承認済みテンプレートの導入を拒否し、レビュープロセスを最初からやり直すことができます。

ワークフローはスキーマレベルではなくテンプレートレベルで実行されるため、各テンプレートを個別に設定、確認、承認できます。



- (注) レビューと承認のワークフローは、Nexus Dashboard で定義されたユーザ ロールに依存するため、この機能を使用するには、Nexus Dashboard リリース 2.1(1) 以降を実行する必要があります。Nexus Dashboard リリース 2.0.2 で Nexus Dashboard Orchestrator を展開した場合、プラットフォームをアップグレードするまで、確認と承認の機能は無効になります。

テンプレート承認要件の有効化

テンプレートの設定と展開に確認と承認のワークフローを使用するには、Nexus Dashboard Orchestrator のシステム設定でこの機能を有効にする必要があります。

-
- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左側のナビゲーションメニューで、[インフラストラクチャ (Infrastructure)] > [システムの設定 (System Configuration)] を選択します。
- ステップ 3** [変更制御 (Change Control)] タイルで、[編集 (Edit)] アイコンをクリックします。
- ステップ 4** [変更制御 (Change Control)] ウィンドウで、[変更制御ワークフロー (Change Control Workflow)] チェックボックスをオンにして機能を有効にします。
- ステップ 5** [承認者 (Approvers)] フィールドに、テンプレートを展開する前に必要な一意の承認の数を入力します。
- ステップ 6** [保存 (Save)] をクリックして、変更内容を保存します。
-

必要なロールを持つユーザの作成

テンプレートの設定と展開のため、レビューと承認のワークフローを実施する前に、NDO サービスが展開されている Nexus ダッシュボードで必要な権限を持つユーザーを作成する必要があります。

-
- ステップ 1** Nexus Dashboard の GUI にログインします。

NDO GUI でユーザーを作成または編集することはできません。サービスが展開されている Nexus ダッシュボード クラスターに直接ログインする必要があります。

- ステップ 2** 左のナビゲーションメニューから、[管理 (Administrative)] > [ユーザー (Users)] を選択します。
- ステップ 3** 必要なユーザーを作成します。

ワークフローは、テンプレート設計者、承認者、および展開者という 3 つの異なるユーザー ロールに依存します。各ロールを異なるユーザーに割り当てることも、同じユーザーにロールの組み合わせを割り当てることもできます。管理者権限を持つユーザは、3 つのアクションすべてを実行できます。

Nexus ダッシュボードにはデザイナー ロールが事前定義されていないため、デザイナーの職務は、デフォルトの管理者ユーザー ロールに加えて、書き込み権限を持つテナント マネージャまたはサイト マネージャユーザーに割り当てられます。

- テナント マネージャは、デザイナーが特定のテナント(またはテナントのサブセット)にのみ関連付けられているテンプレートに変更を加える必要がある場合に使用する必要があります。この場合、ユーザーを特定のテナントにマッピングする必要があります。
- デザイナーが異なるテナントに属するテンプレートに変更を加える必要がある場合は、サイト マネージャを使用する必要があります。

デザイナーの役割とは対照的に、Nexus ダッシュボードには、ユーザーに関連付けることができる事前定義された承認者および展開者の役割があります。承認者および展開者のロールは、設計上、特定のテナントにバインドされていません。ただし、デザイナーと承認者(またはデザイナーとデプロイヤー)の両方の権限を持つユーザー ロールを作成する場合は、上記と同じガイドラインに従ってください。

ローカルまたはリモートの Nexus ダッシュボード ユーザーのユーザーとその権限の設定の詳細については、『[Nexus Dashboard User Guide](#)』を参照してください。

承認者ロールを持つ別個のユーザーが、[テンプレート承認要件の有効化 \(54 ページ\)](#) で設定した承認の最小数と同数以上必要です。

(注) **変更制御ワークフロー機能を無効にすると**、承認者と展開者のユーザーは Nexus Dashboard Orchestrator に読み取り専用でアクセスできます。

テンプレートのレビューと承認の要求

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものがが必要です。

- 承認要件のグローバル設定を有効にした ([テンプレート承認要件の有効化 \(54 ページ\)](#) を参照)。
- 承認者ロールと展開者ロールを使用して Nexus ダッシュボードでユーザーを作成または更新した ([必要なロールを持つユーザーの作成 \(54 ページ\)](#) を参照)。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。

ステップ 1 テナント マネージャ、サイト マネージャ、または管理者ロールを持つユーザーとして Nexus Dashboard Orchestrator GUI にログインします。

ステップ 2 テナント マネージャ ロールを割り当てた場合は、ユーザーをテナントに関連付けます。

サイト マネージャ または 管理者 ロールを使用していた場合は、この手順をスキップしてください。

テナント マネージャ ロールを割り当てる場合は、ユーザーが管理する特定のテナントにユーザーを関連付ける必要もあります。

- a) 左型のナビゲーションメニューから、[アプリケーション管理 (Application Management)] > [テナント (Tenants)] を選択します。
- b) ユーザーが管理するテナントを選択します。
- c) Nexus Dashboard で作成したデザイナー ユーザーの横にあるチェックボックスをオンにします。
- d) ユーザーが管理する他のすべてのテナントについて、この手順を繰り返します。

ステップ 3 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 4 承認を要求するテンプレートを含むスキーマをクリックします。

ステップ 5 スキーマビューで、テンプレートを選択します。

ステップ 6 メイン ペインで、**[承認のために送信 (Send for Approval)]** をクリックします。

[承認のために送信 (Send for Approval)] ボタンは、次の場合には使用できません。

- グローバル変更制御オプションが有効になっていない
- テンプレートにポリシー設定がないか、どのサイトにも割り当てられていない
- ユーザにテンプレートを編集する権限がない
- テンプレートは承認のためにすでに送信されている
- テンプレートが承認者ユーザによって拒否された

テンプレートのレビューと承認

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものがが必要です。

- 承認要件のグローバル設定を有効にした ([テンプレート承認要件の有効化 \(54 ページ\)](#) を参照)。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した ([必要なロールを持つユーザの作成 \(54 ページ\)](#) を参照)。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。
- [テンプレートのレビューと承認の要求 \(55 ページ\)](#) に記載されているように、スキーマエディタによってテンプレートの承認が要求されました。

ステップ 1 承認者 (Approver) または管理者 (admin) ロールを持つユーザとして Nexus Dashboard Orchestrator GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、**[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)]** を選択します。

ステップ 3 確認して承認するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマビューで、テンプレートを選択します。

ステップ 5 メインペインで、**[承認 (Approve)]** をクリックします。

すでにテンプレートを承認または拒否している場合は、テンプレートデザイナーが変更を行い、再確認のためにテンプレートを再送信するまで、このオプションは表示されません。

ステップ 6 [テンプレートの承認 (Approving template)] ウィンドウでテンプレートを確認し、[承認 (Approve)] をクリックします。

承認画面には、テンプレートがサイトに展開するすべての変更が表示されます。

[バージョン履歴の表示 (View Version History)] をクリックすると、完全なバージョン履歴と、バージョン間で行われた増分変更を表示できます。バージョン履歴の詳細については、[履歴の表示と以前のバージョンの比較 \(49 ページ\)](#) を参照してください。

[展開計画 (Deployment Plan)] をクリックして、このテンプレートから展開される設定の可視化と XML を表示することもできます。[展開計画 (Deployment Plan)] ビューの機能は、[現在展開されている設定の表示 \(72 ページ\)](#) で説明した、すでに導入されているテンプレートの [展開ビュー (Deployed View)] に似ています。

テンプレートの展開

ここでは、新しいポリシーまたは更新されたポリシーを ACI ファブリックに展開する方法について説明します。

始める前に

このドキュメントの前のセクションで説明したように、作成されたサイトには、展開するスキーマ、テンプレート、およびオブジェクトが必要です。

[テンプレートのレビューと承認 \(53 ページ\)](#) で説明しているように、テンプレートの確認と承認が有効になっている場合は、必要な数の承認者によってテンプレートがすでに承認されている必要があります。

ステップ 1 展開するテンプレートを含むスキーマに移動します。

ステップ 2 左側のサイドバーで、展開するテンプレートを選択します。

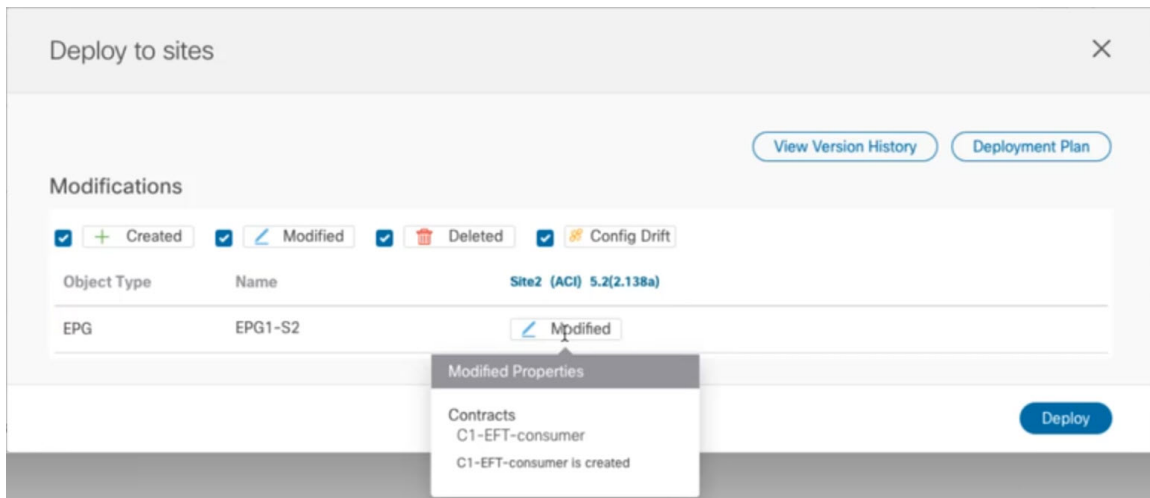
ステップ 3 テンプレート編集ビューの右上で、[展開 (Deploy)] をクリックします。

[サイトに展開 (Deploy to Sites)] ウィンドウが開き、展開するオブジェクトの概要が表示されます。

ステップ 4 テンプレートに変更を加えた場合は、[展開の計画 (Deployment Plan)] を確認して新しい構成を確認します。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、[展開] の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

[サイトに展開 (Deploy to Sites)] ウィンドウには、サイトに展開される構成の違いの概要が表示されます。次のスクリーンショットは、サイト 2 の既存の EPG (EPG1-S2) にコンシューマコントラクトを追加する簡単な例を示しています。



情報目的で [作成日 (Created)]、[変更日 (Modified)]、および [削除済み (Deleted)] チェックボックスを使用してビューをフィルタリングすることもできますが、**[展開 (Deploy)]** をクリックするとすべての変更が展開されることに注意してください。

ここでは、次のことも選択できます。

- **[バージョン履歴の表示 (View Version History)]** を選択すると、完全なバージョン履歴とバージョンアップグレードで行われた更新内容を表示します。バージョン履歴の詳細については、[履歴の表示と以前のバージョンの比較 \(49 ページ\)](#) を参照してください。
- **[展開プラン (Deployment Plan)]** を確認して、このテンプレートから展開される構成の可視化と XML ペイロードを表示します。

この機能により、テンプレートに変更を加えて 1 つ以上のサイトに展開した後に、Orchestrator がマルチサイトドメインの一部であるさまざまなファブリックにプロビジョニングする構成の変更を、より適切に可視化できます。

テンプレートとサイト構成に加えられた特定の変更のリストを引き続き提供していた **Multi-Site Orchestrator** の以前のリリースとは異なり、展開プランでは、テンプレートの展開によってさまざまなファブリック全体にプロビジョニングされる、すべてのオブジェクトに対する完全な可視性が提供されます。たとえば、変更内容によっては、特定の変更が 1 つのサイトのみに適用された場合でも、シャドウオブジェクトが複数のサイトに作成される場合があります。

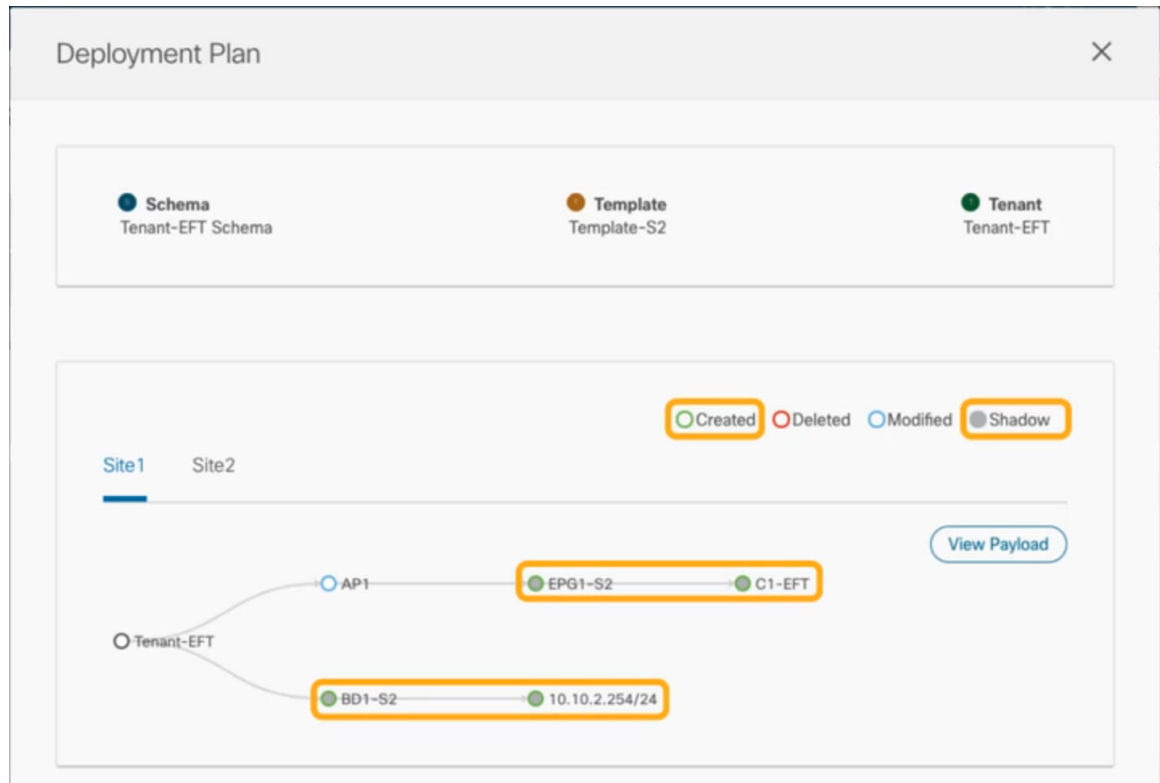
(注) テンプレートを展開する前に、この手順で説明されているように、展開プランを使用して変更を確認することをお勧めします。構成変更の視覚的に示すことは、意図しない構成変更の展開による潜在的なエラーを低減するのに役立ちます。

- a) **[展開プラン (Deployment Plan)]** ボタンをクリックします。

前のステップで示したのと同じ例で続けると、コンシューマコントラクトがサイト 2 の既存の EPG に追加され、展開計画では、サイト 2 への変更の結果として、サイト 1 に展開される追加の変更があることも確認できます。

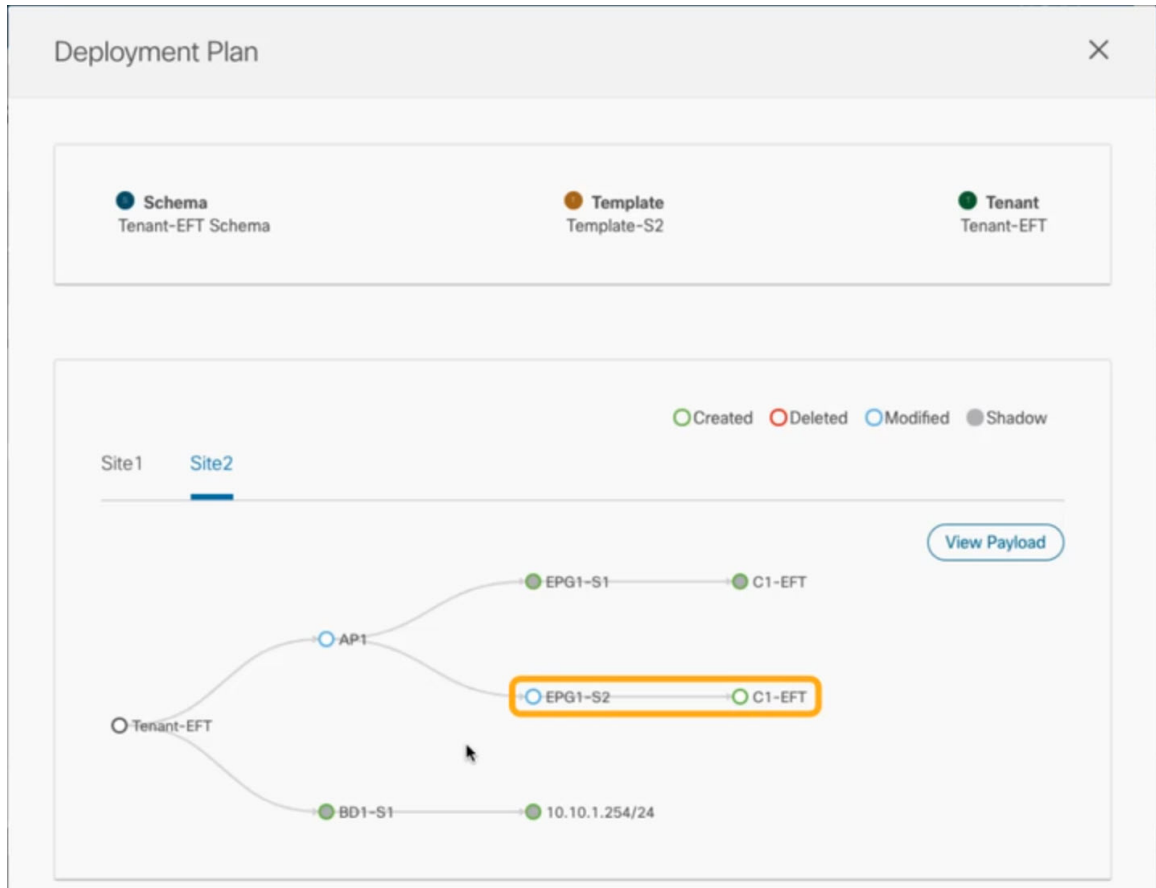
- b) 最初にリストされたサイトで変更を確認します。

強調表示された凡例に基づいて、Orchestrator がサイト 2 の EPG に追加したコントラクトに必要なシャドウ オブジェクトをサイト 1 に作成することがわかります。



- c) 前のサブステップを繰り返して、他のサイトの変更を確認します。

ここでは、コントラクト (C1-EFT) をサイト 2 に割り当てたときに、サイト 2 の EPG (EPG1-S2) に明示的に加えた変更と、そのコントラクトを提供している他のサイトの EPG (EPG1-S1) のシャドウ オブジェクトを確認できます。



- d) (オプション) [ペイロードの表示 (View Payload)] をクリックすると、各サイトの XML ペイロードを表示できます。

新規および変更されたオブジェクトの視覚的表現に加えて、各サイトの変更について [ペイロードの表示 (View Payload)] を選択することもできます。

```

<polUni>
  <fvTenant name="Tenant-EFT" annotation="orchestrator:msc">
    <fvAp name="AP1" annotation="orchestrator:msc-shadow:no">
      <fvAEPg name="EPG1-S2" isAttrBasedEpg="no" pcEnfPref="unenforced" fwdCtrl="" prefGrMemb="exclude" hasMcastSource="no"
        prio="unspecified" annotation="orchestrator:msc-shadow:yes">
        <fvRsBd tnFvBDName="BD1-S2"/>
        <fvRsCons tnVzBrCPName="C1-EFT" annotation="orchestrator:msc">
        </fvRsCons>
        <fvSiteAssociated sitelid="1" name="msc-local">
        </fvSiteAssociated>
      </fvAEPg>
    </fvAp>
    <fvBD name="BD1-S2" arpFlood="yes" intersiteBumTrafficAllow="no" OptimizeWanBandwidth="no" unkMacUcastAct="proxy"
      intersiteL2Stretch="no" mcastAllow="no" hostBasedRouting="no" vmac="not-applicable" mac="00:22:BD:F8:19:FF"
      unkMcastAct="flood" v6unkMcastAct="flood" multiDstPktAct="bd-flood" unicastRoute="yes" annotation="orchestrator:msc-
      shadow:yes">
      <fvRsCtx tnFvCtxName="VRF1"/>
      <fvSubnet ip="10.10.2.254/24" scope="private" descr="" ctrl="no-default-gateway" virtual="no" preferred="no"
        annotation="orchestrator:msc-shadow:no">
      </fvSubnet>
      <fvSiteAssociated sitelid="1" name="msc-local">
      </fvSiteAssociated>
    </fvBD>
  </fvTenant>
</polUni>

```

- e) 変更の確認が完了したら、[x] アイコンをクリックして [展開プラン (Deployment Plan)] 画面を閉じます。

ステップ 5 [サイトに展開 (Deploy to sites)] ウィンドウで、[展開 (Deploy)] をクリックしてテンプレートを展開します。

テンプレートの展開解除

ここでは、サイトからテンプレートを展開解除する方法について説明します。

始める前に

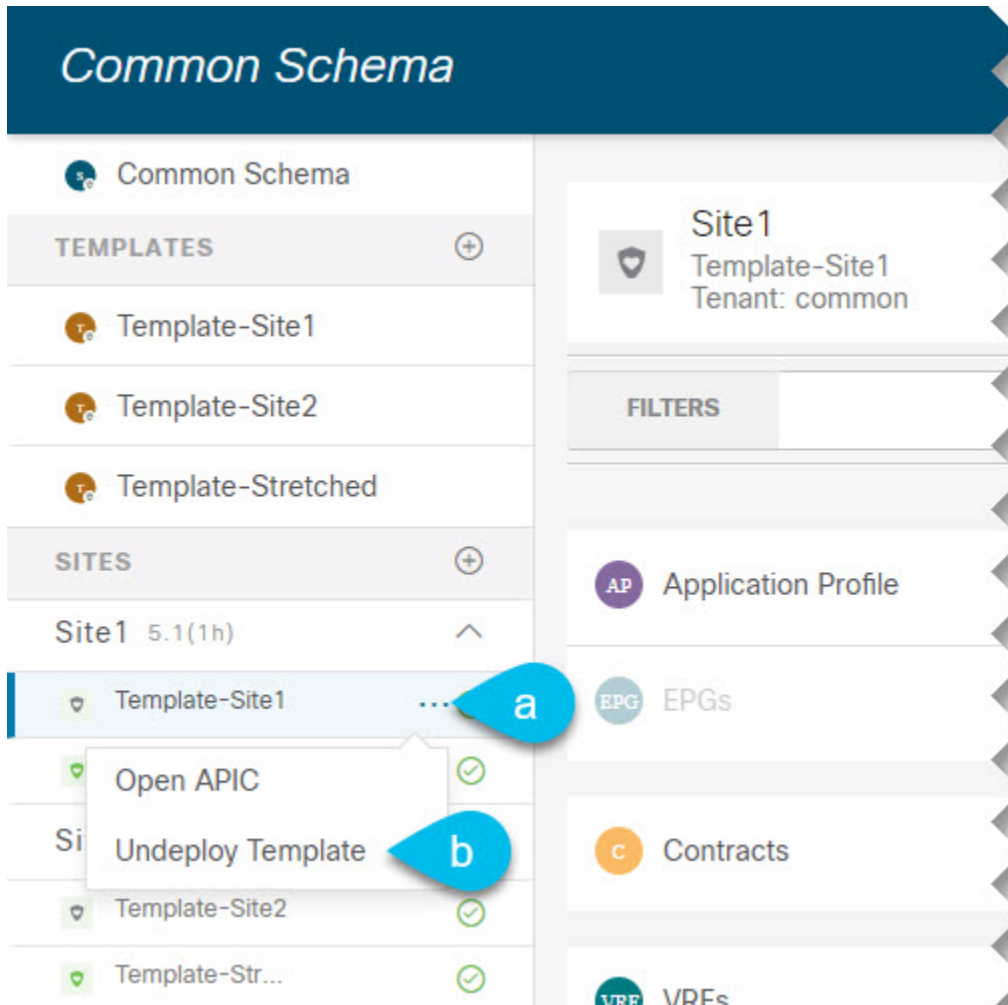
- テンプレートを最後に展開してから、テンプレートに変更を加えていないことを確認します。

最後に展開された後に変更されたテンプレートを展開解除すると、テンプレートに展開されたオブジェクトのセットが、テンプレートに変更を加えた後に展開解除しようとするオブジェクトのセットと異なるため、設定がずれる可能性があります。

ステップ 1 展開解除するテンプレートを含むスキーマを選択します。

ステップ 2 [サイト (SITES)] の下の左側のサイドバーで、展開を解除するテンプレートを選択します。

ステップ3 テンプレートを展開解除します。



- a) テンプレートの横にある [その他のオプション (More options) (...)] メニューをクリックします。
- b) [テンプレートの展開解除 (Undeploy Template)] をクリックします。

サイトからのテンプレートの関連付け解除

展開を解除せずに、サイトからテンプレートの関連付けを解除することもできます。これにより、NDO からサイトに展開された設定を保持しながら、スキーマのテンプレートとサイトの関連付けを削除できます。管理対象オブジェクトとポリシーの所有権が NDO からサイトのコントローラに移されます。

始める前に

- テンプレートとその設定がサイトにすでに展開されている必要があります。

- テンプレートは、単一のサイトにのみ展開し、サイト間で展開しないようにする必要があります。
- テンプレートで定義されたオブジェクトは、他のサイトのシャドウオブジェクトとして展開しないでください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 関連付けを解除するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマ ビューで、関連付けを解除する特定のサイトの下のテンプレートを選択します。

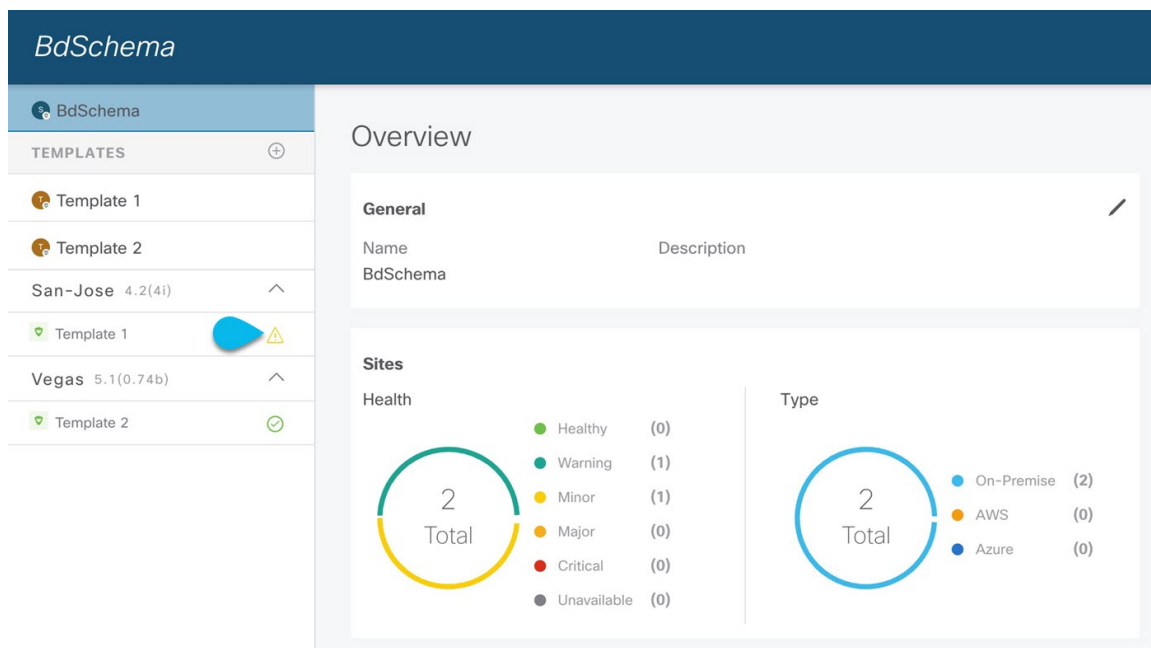
ステップ 5 [アクション (Actions)] メニューから [テンプレートの関連付け解除 (Disassociate Template)] を選択します。

ステップ 6 確認ウィンドウで、[アクションの確認 (Confirm Action)] をクリックします。

設定のばらつき

APIC ドメインに実際に展開された設定が、Nexus Dashboard Orchestrator でそのドメインに対して定義された設定と異なる場合があります。これらの構成の不一致は、[構成のばらつき (Configuration Drifts)] と呼ばれ、次の図に示すように、スキーマ ビューのテンプレート名の横に黄色の注意サインで示されます。

図 5:



設定のばらつきは、さまざまな理由で発生する可能性があります。構成のばらつきを解決するために必要な実際の手順は、その原因によって異なります。最も一般的なシナリオとその解決策を次に示します。

- **NDO で設定が変更された** : NDO GUIでテンプレートを変更すると、変更をサイトに展開するまでは、設定のばらつきとして表示されます。
このタイプの設定のずれを解決するには、テンプレートを展開して変更をサイトに適用するか、スキーマの変更を元に戻します。
- **設定がサイトの APIC で直接変更された** : NDO から展開されたオブジェクトは、サイトの APIC で警告アイコンとテキストで示されます。管理ユーザー、設定のずれの原因に対し、引き続き変更を加えられます。



(注) APIC でオブジェクトが変更されるたびに、APIC は Nexus Dashboard Orchestrator に通知を送信します。通知を受信すると、Nexus Dashboard Orchestrator は 30 秒のタイマーを開始し（さらに通知が届くのを待ちます）、そのようなタイマーの期限が切れると、APIC への API 呼び出しを実行して、通知を受信したすべてのオブジェクトに加えられた変更に関する詳細情報を取得します。これにより、Nexus Dashboard Orchestrator は、それらのオブジェクトが定義されているすべてのテンプレートの UI にばらつきのシンボルを表示できます。この動作の唯一の例外は、Nexus Dashboard Orchestrator が、特定のテンプレートで定義されたオブジェクトのすべて（またはそのサブセット）の構成を展開する場合です。その場合、60 秒間、Nexus Dashboard Orchestrator は、それらの特定のオブジェクトに関して APIC から受信した通知を無視し、その結果、UI にばらつきのシンボルを表示できません。

- **NDO 設定がバックアップから復元された** : NDO のバックアップから設定を復元すると、バックアップが作成されたときのオブジェクトとその状態のみが復元され、復元された設定は自動的に再展開されません。そのため、バックアップが作成されてから構成に変更が加えられ、APIC に展開された場合、バックアップを復元すると構成のばらつきが作成される可能性があります。
- **NDO 設定は、古いリリースで作成されたバックアップから復元された** : 新しいリリースで、以前のリリースではサポートされていなかったオブジェクトプロパティのサポートが追加された場合、これらのプロパティによって設定がずれる可能性があります。通常、これは、サイトの APIC GUI で新しいプロパティが直接変更され、Nexus Dashboard Orchestrator の想定値がデフォルトと異なる場合に発生します。
- **NDO が以前のリリースからアップグレードされた** : このシナリオは、新しいオブジェクトプロパティが新しいリリースに追加された場合に、既存の設定がずれている可能性がある、前のシナリオと似ています。

NDO リリース 3.6(1) 以降、テンプレートに対して「ばらつきの調整」ワークフローを実行して、ばらつきの原因をより詳細に把握し、ばらつきを調整できるようにすることを

勧めします。この推奨事項は、このセクションで前述したすべてのばらつきのシナリオに適用されます。NDO 3.6 の新しいばらつきの調整ワークフローの詳細については、以下の「構成のばらつきの調整」セクションを参照してください。

設定のばらつきの調整

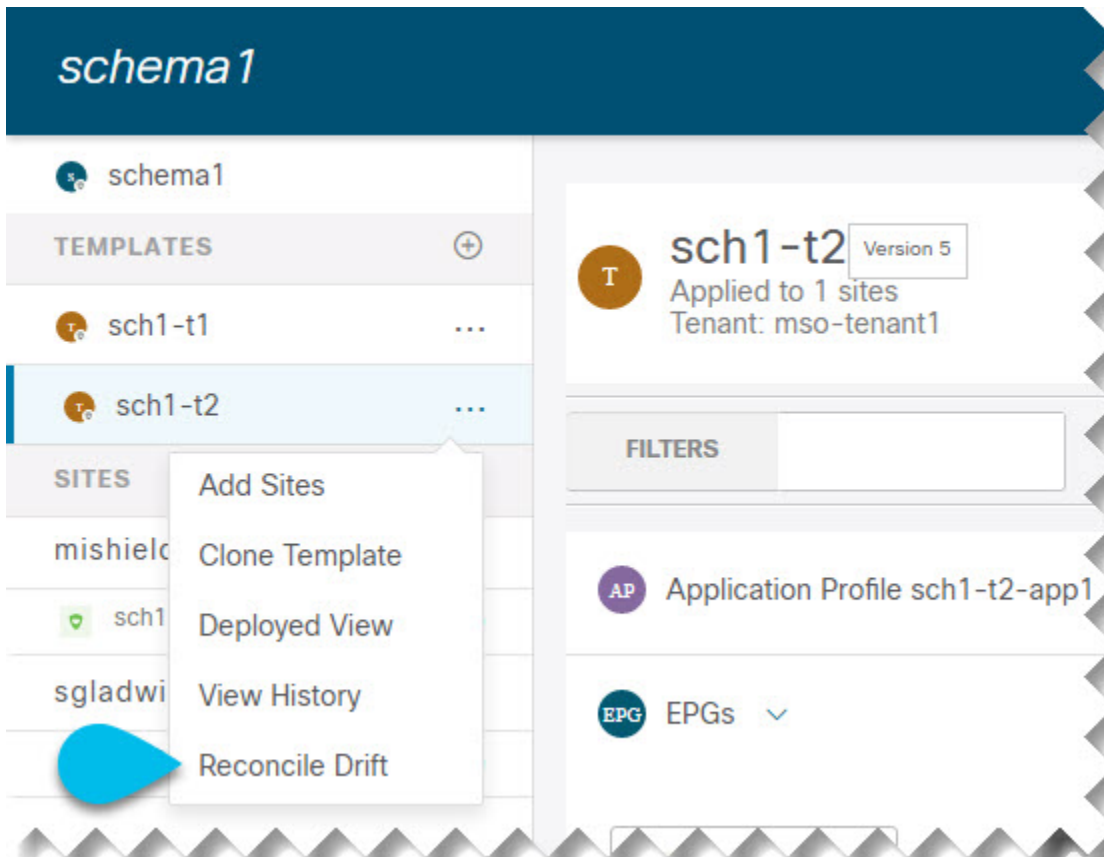
NDO リリース 3.6(1) では、Nexus Dashboard Orchestrator で定義されたテンプレート構成と、マルチサイトドメインのサイト部分の APIC コントローラーでレンダリングされた構成を比較するために実行できるばらつき調整ワークフローのサポートが導入されています。これにより、構成のばらつき（つまり、Nexus Dashboard Orchestrator または APIC で直接行われた変更）の原因をより明確に把握でき、以下の手順で説明するように、ばらつきを調整する方法をユーザーに選択させることができます。



-
- (注) 選択した構成が必要ない場合は、スキーマを閉じて再度開くことができます。これにより、元の構成が表示されます。必要に応じて、「Reconcile Drift」フローを再度トリガーできます。[保存 (Save)] または [展開 (Deploy)] ボタンを選択した後にのみ、スキーマが保存されます。
-

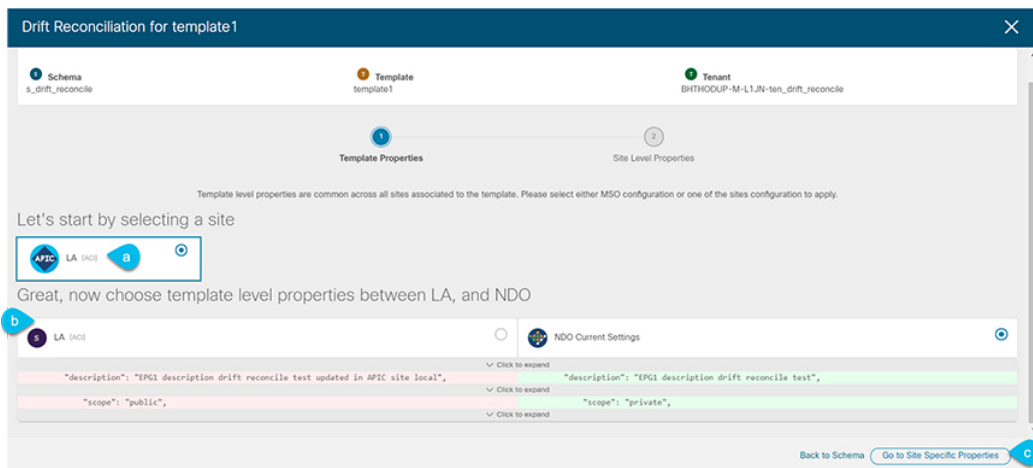
ステップ 1 設定のばらつきを確認するテンプレートを含むスキーマに移動します。

ステップ 2 テンプレートの [アクション (Actions)] メニューから、[ばらつきの調整 (Reconcile Drift)] を選択します。



[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

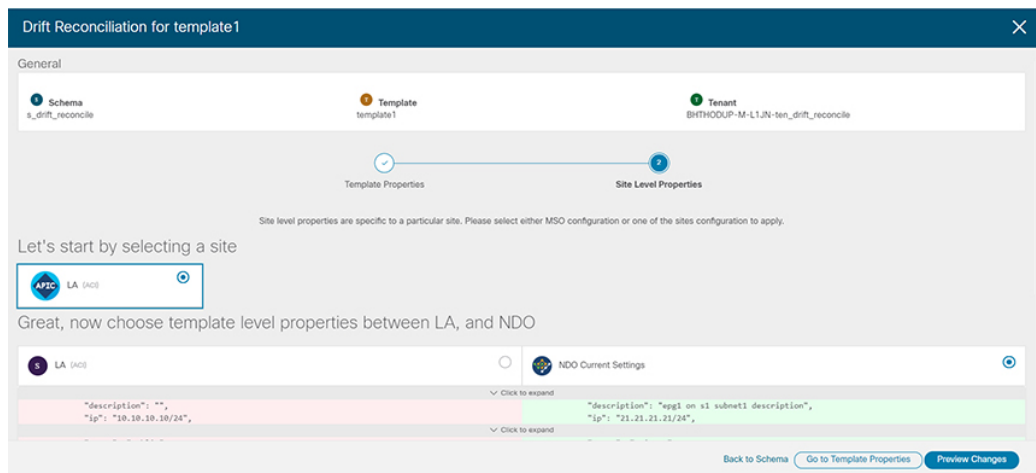
ステップ 3 [ばらつきの調整 (Reconcile Drift)] 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレートレベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成を

選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変更されますが、Nexus Dashboard Orchestrator 構成を選択した場合は、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま保持されます。

ステップ 4 [サイト固有のプロパティに移動 (Go to Site Specific Properties)] をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカルプロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルの構成とサイトレベルの構成のどちらでも同じ選択を行います。ばらつきの調整ウィザードでは、サイトのコントローラで定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

ステップ 5 [変更のプレビュー (Preview Changes)] をクリックして、選択内容を確認します。

プレビューは [ばらつきの調整 (Reconcile Drift)] ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、[サイトに展開 (Deploy to site)] をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

スキーマの複製

このセクションでは、[スキーマ (Schemas)] 画面の [スキーマの複製 (Clone Schema)] 機能を使用して、既存のスキーマとそのすべてのテンプレートのコピーを作成する方法について説明します。

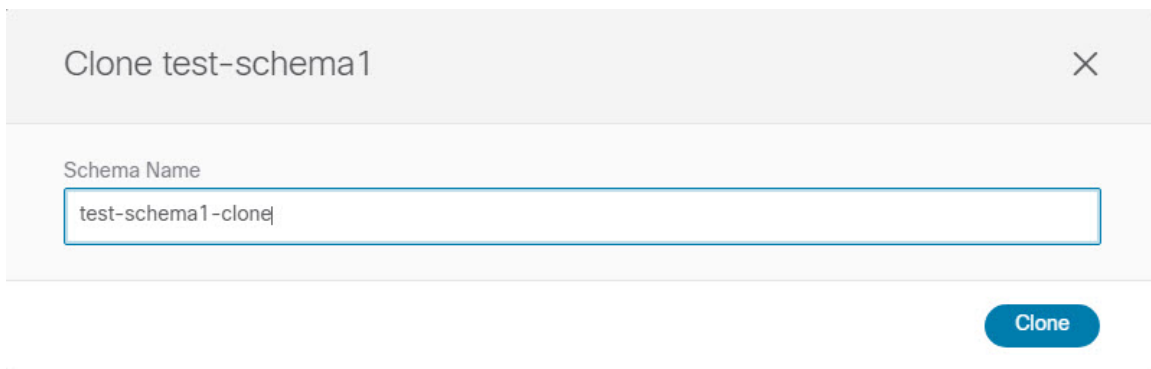
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 複製するスキーマを選択します。

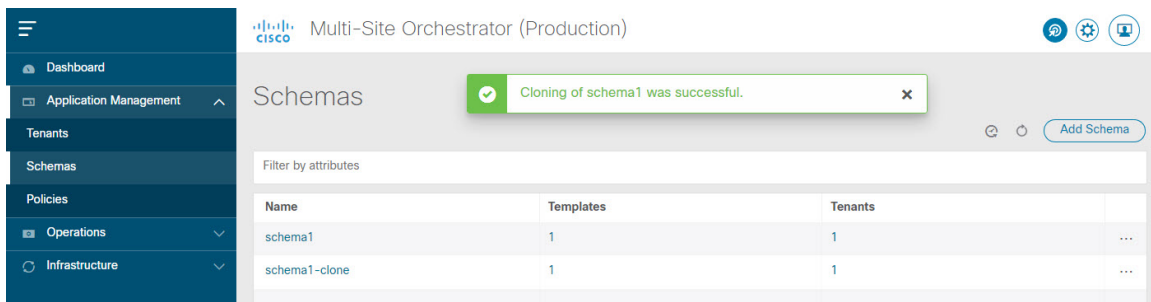


- a) 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。
- b) 複製するスキーマ名の横にある [アクション (Actions)] メニューから、[スキーマの複製 (Clone Schema)] を選択します。

ステップ 3 新しいスキーマの名前を入力し、[複製 (Clone)] をクリックします。



[複製 (Clone)] をクリックすると、UI に [<スキーマ名の複製に成功しました (Cloning of <schema-name> was successful)] というメッセージが表示され、新しいスキーマが [スキーマ (Schemas)] 画面に表示されます。

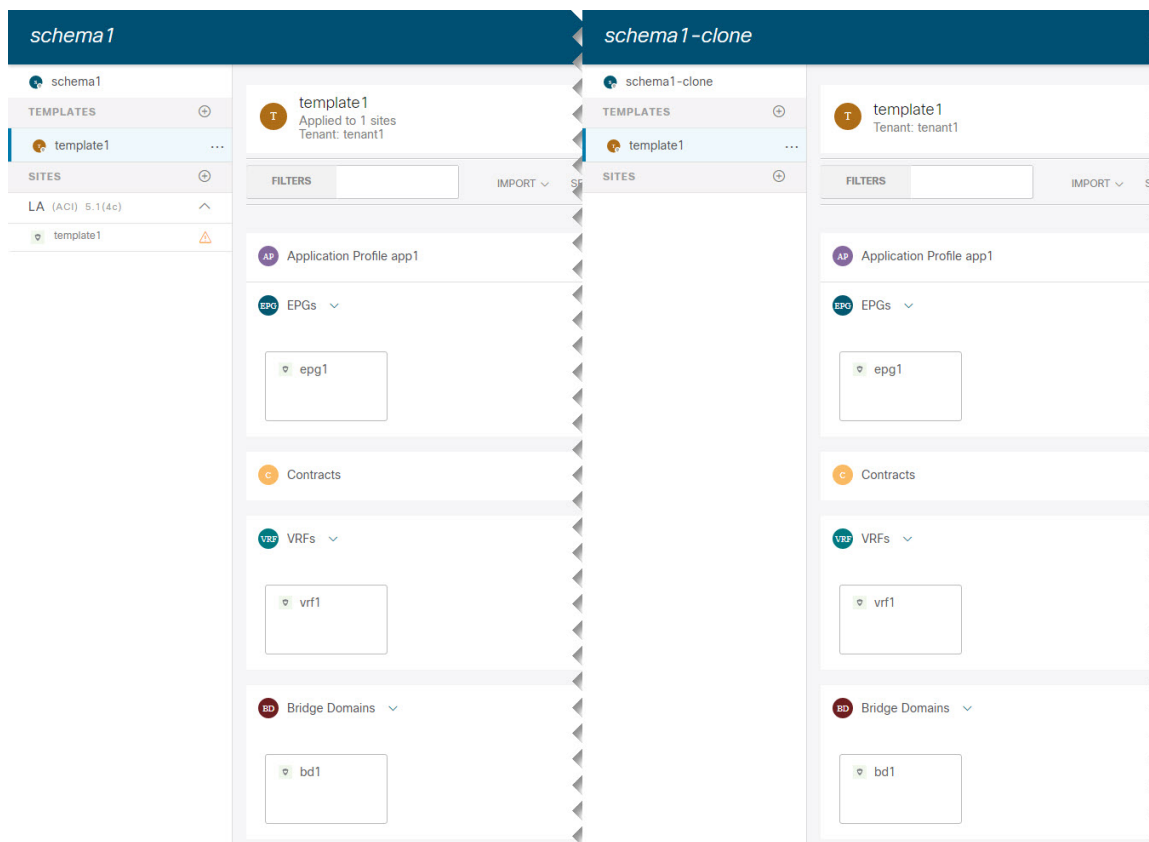


新しいスキーマは、元のスキーマとまったく同じテンプレート（およびそのテナントの関連付け）、オブジェクト、およびポリシー設定で作成されます。

テンプレート、オブジェクト、および設定はコピーされますが、サイトの関連付けは保持されないため、それらを展開するサイトに複製されたスキーマのテンプレートを再度関連付ける必要があります。同様に、テンプレートオブジェクトをサイトに関連付けた後に、テンプレートオブジェクトのサイト固有の設定を指定する必要があります。

ステップ 4 (オプション) スキーマとそのすべてのテンプレートがコピーされたことを確認します。

2つのスキーマを比較することで、操作が正常に完了したことを確認できます。



テンプレートの複製

ここでは、スキーマ ビューで [テンプレートの複製 (Clone Template)] 機能を使用して既存のテンプレートのコピーを作成する方法について説明します。

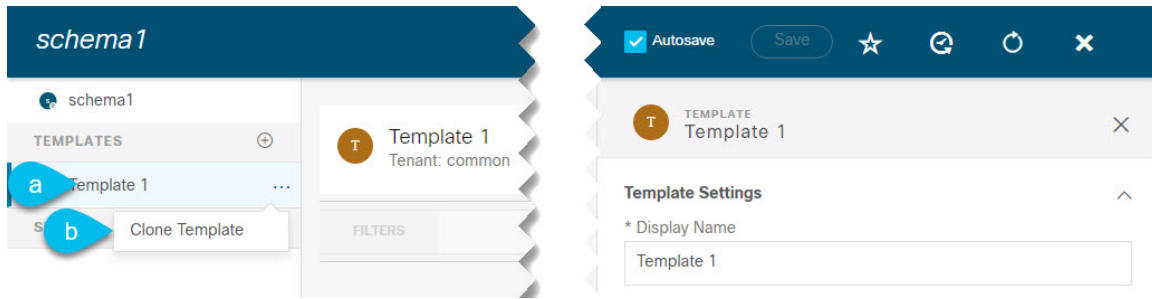
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 複製するテンプレートを含むスキーマをクリックします。

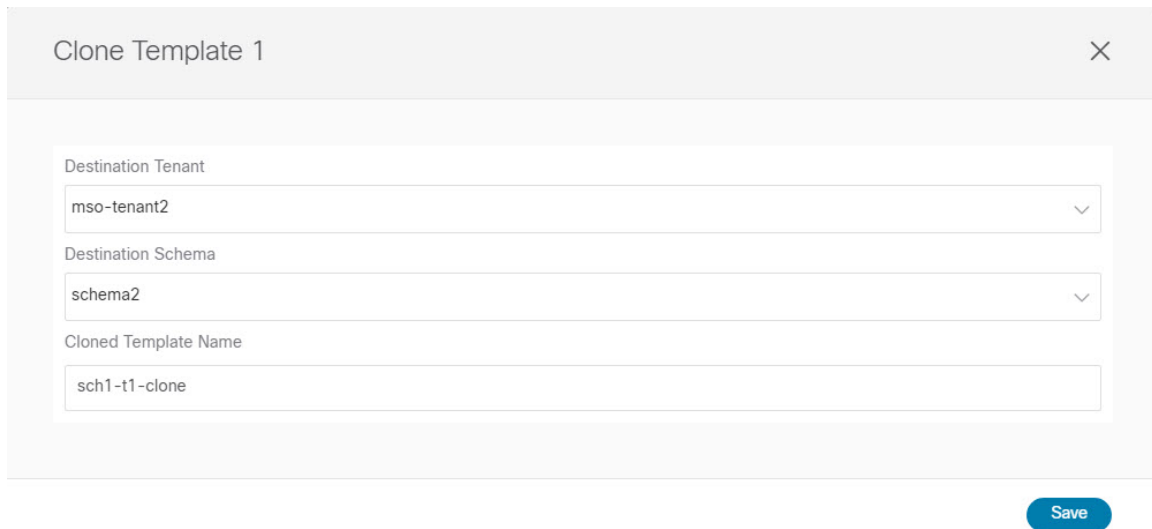
■ テンプレートの複製

ステップ4 [スキーマ (Schema)] ビューで、[テンプレートのクローン (Clone Template)] ダイアログを開きます。



- a) 複製するテンプレートを選択します。
- b) [アクション (Actions)] メニューから [テンプレートのクローン (Clone Template)] を選択します。

ステップ5 クローンの複製先の詳細を入力します。



- a) **[複製先テナント (Destination Tenant)]** ドロップダウンから、ターゲットテナントを選択します。
デフォルトでは、現在のテンプレートのテナントが選択されています。テナントを変更すると、代わりに新しいテンプレートが選択したテナントに割り当てられます。
複製先テナントはすでに存在している必要があります。テンプレートを複製して新しいテナントに割り当てる場合は、まず[テナント (Tenants)] ページでテンプレートを作成してから、テンプレートに戻って複製する必要があります。
(注) 異なるテナント間で複製する場合、他のテンプレートのオブジェクトを参照するオブジェクトをテンプレートに含めることはできません。
- b) **[複製先スキーマ (Destination Schema)]** ドロップダウンから、テンプレートのクローンを作成するスキーマの名前を選択します。
このテンプレートのクローンを含めるために、同じスキーマまたは異なるスキーマを選択できます。まだ存在しないスキーマにテンプレートを複製する場合は、スキーマの名前を入力し、[作成 (Create) <schema-name>] オプションを選択して新しいスキーマを作成できます。

(注) 異なるスキーマ間で複製する場合、テンプレートには他のテンプレートのオブジェクトを参照するオブジェクトを含めることはできません。

- c) [テンプレート名 (Template Name)] フィールドに、テンプレートの名前を入力します。
- d) [保存 (Save)] をクリックして、クローンを作成します。

新しいテンプレートが、選択したテナントと元のテンプレートとまったく同じオブジェクトおよびポリシー設定で複製先スキーマに作成されます。

選択した複製先スキーマがソーステンプレートと同じスキーマである場合、スキーマビューがリロードされ、新しいテンプレートが左側のサイドバーに表示されます。別のスキーマを選択した場合は、そのスキーマに移動して新しいテンプレートを表示および編集できます。

テンプレート オブジェクトと設定はコピーされますが、サイトの関連付けは保持されないため、複製したテンプレートを展開するサイトに再度関連付ける必要があります。同様に、テンプレートオブジェクトをサイトに関連付けた後に、テンプレート オブジェクトのサイト固有の設定を指定する必要があります。

テンプレート間でのオブジェクトの移行

ここでは、テンプレートまたはスキーマ間でオブジェクトを移動する方法について説明します。1つ以上のオブジェクトを移動すると、次の制約事項が適用されます。

- テンプレート間で移動できるのは、EPG および Bridge Domain (BD) オブジェクトのみです。
- クラウド APIC サイトとの間でのオブジェクトの移行はサポートされていません。オンプレミスサイト間でのみオブジェクトを移行できます。
- 送信元と宛先のテンプレートは同じスキーマにも異なるスキーマにもすることができますが、テンプレートは同じテナントに割り当てる必要があります。
- 宛先テンプレートが作成され、少なくとも1つのサイトに割り当てられている必要があります。
- 宛先テンプレートが展開されておらず、他のオブジェクトがない場合、そのテンプレートは、オブジェクトの移行後に自動的に展開されます。
- 1つのオブジェクト移行を開始すると、同じ送信元またはターゲットテンプレートを含む別の移行を実行することはできません。テンプレートがサイトに展開されると、移行が完了します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから [スキーマ(Schemas)] を選択します。

現在展開されている設定の表示

- ステップ 3** 移行するオブジェクトが含まれているスキーマをクリックします。
- ステップ 4** [スキーマ (Schema)] ビューで、移行するオブジェクトが含まれているテンプレートを選択します。
- ステップ 5** メインペインの右上にある **[選択 (Select)]** をクリックします。
これにより、移行する 1 つ以上のオブジェクトを選択できます。
- ステップ 6** 移行する各オブジェクトをクリックします。
選択したオブジェクトには、右上隅にチェックマークが表示されます。
- ステップ 7** メインペインの右上にある [アクション (actions)] (...) アイコンをクリックし、**[オブジェクトの移行 (Migrate Objects)]** を選択します。
- ステップ 8** **[オブジェクトの移行 (Migrate objects)]** ウィンドウで、オブジェクトを移動する宛先スキーマとテンプレートを選択します。
リストには、少なくとも 1 つのサイトが接続されているテンプレートのみが表示されます。ドロップダウンリストにターゲットテンプレートが表示されない場合は、ウィザードをキャンセルし、そのテンプレートを少なくとも 1 つのサイトに割り当てます。
- ステップ 9** **[OK]** をクリックし、**[はい (YES)]** をクリックしてオブジェクトを移動することを確認します。
オブジェクトは、ソーステンプレートから選択した宛先テンプレートに移行されます。設定を展開すると、ソーステンプレートが展開され、宛先テンプレートが展開されているサイトに追加されるサイトから、オブジェクトが削除されます。
- ステップ 10** 移行が完了したら、ソースと宛先の両方のテンプレートを再展開します。
宛先テンプレートが展開されておらず、他のオブジェクトがない場合、そのテンプレートはオブジェクトの移行後に自動的に展開されるため、この手順をスキップできます。

現在展開されている設定の表示

特定のテンプレートからサイトに現在展開されているすべてのオブジェクトを表示できます。任意のテンプレートを何度でも展開、展開解除、更新、および再展開できますが、この機能では、これらすべてのアクションの結果としての最終的な状態のみが表示されます。たとえば、Template1 に VRF1 オブジェクトのみが含まれ、Site1 に展開されている場合、API はそのテンプレートの VRF1 蚤を返します。その後、BD1 を追加して再展開すると、その時点から、API は BD1 と VRF1 の両方のオブジェクトを返すようになります。

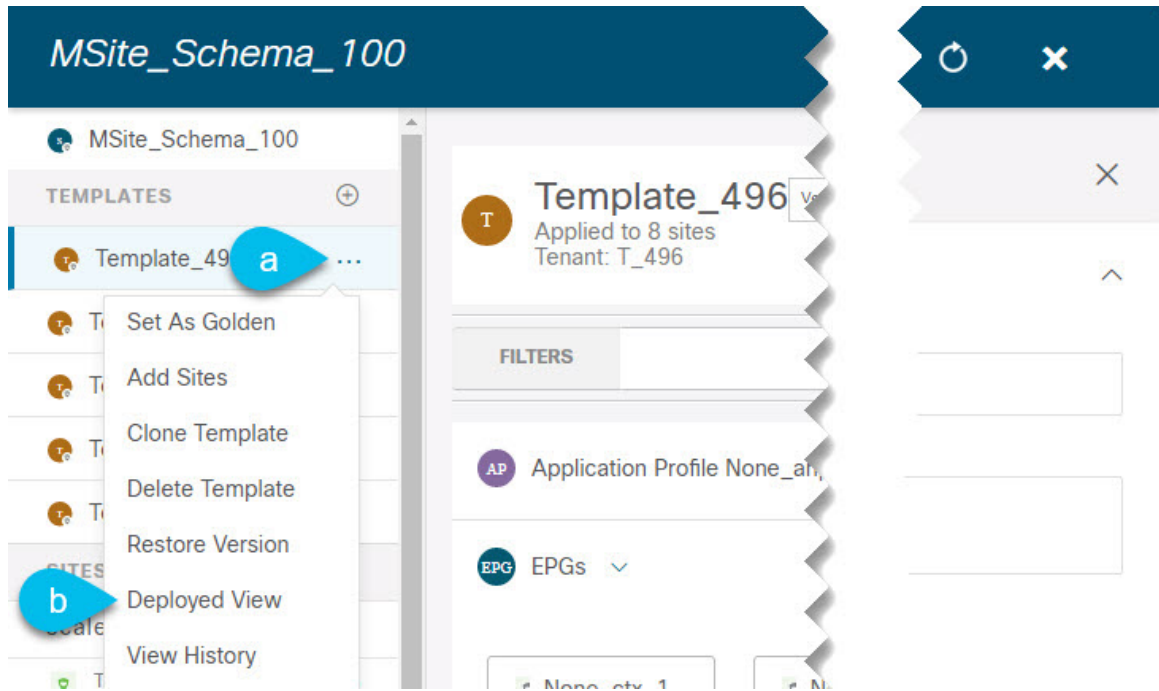
この情報は Orchestrator データベースから取得されるため、サイトのコントローラで直接行われた変更によって発生する可能性のある設定の変動は考慮されません。

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左型のナビゲーションメニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ3 表示するテンプレートを含むスキーマをクリックします。

ステップ4 左側のサイドバーで、テンプレートを選択します。

ステップ5 そのテンプレートの **[展開ビュー (Deployed View)]** を開きます。



a) テンプレートの名前の横にある **[アクション (Actions)]** メニューをクリックします。

b) **[展開ビュー (Deployed View)]** をクリックします。

ステップ6 **[展開ビュー (Deployed View)]** 画面で、情報を表示するサイトを選択します。

サイトにすでに展開されているものと、テンプレートで定義されているものとのテンプレート設定の比較がグラフィカルに表示されます。

Deployment View

Schema	Template	Tenant
MSite_Schema_100	Template_496	

scale-ms11 scale-ms7 scale-ms8 scale-ms6 scale-ms12 scale1 scale-ms9

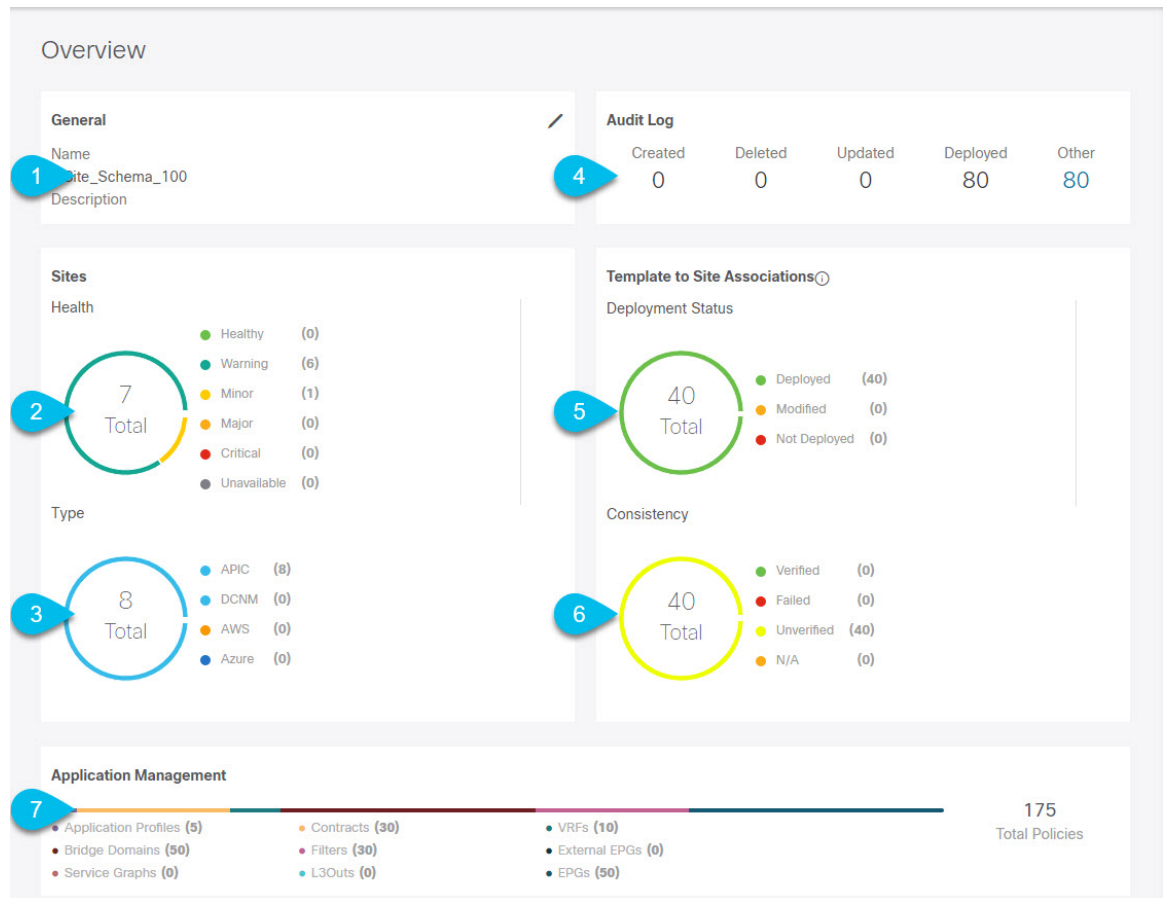
```
<polUni>
  <fvTenant name='T_496' annotation='orchestrator.msc'>
    <fvAp name='None_anp_1' annotation='orchestrator.msc-shadow:no'>
      <fvAEPg name='None_ctx_2_bd_5_epg_1' isAttrBasedEPg='no' fwdCtrl='' prefGrpMemb='exclude'
        hasMcastSource='no' prio='unspecified' annotation='orchestrator.msc-shadow:no'>
        <fvRsBd tnFvBDName='None_ctx_2_bd_5'/>
        <fvRsProv tnVzBrCPName='tenant_ctr_None_ctx_2' annotation='orchestrator.msc'> </fvRsProv>
        <fvRsCons tnVzBrCPName='tenant_ctr_None_ctx_2' annotation='orchestrator.msc'>
        </fvRsCons>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

- 色分けされた凡例は、この時点でテンプレートを展開する場合に作成、削除、または変更されるオブジェクトを示します。
テンプレートの最新バージョンがすでに展開されている場合、ビューには色分けされたオブジェクトは含まれず、現在展開されている設定が表示されます。
- サイト名をクリックすると、その特定のサイトの設定を表示できます。
- [XML/JSON 表示 (View XML/JSON)]** をクリックすると、選択したサイトに展開されているすべてのオブジェクトの XML 設定が表示されます。

スキーマの概要と展開ビジュアライザ

1つ以上のオブジェクトが定義され、1つ以上のACIファブリックに展開されたスキーマを開くと、スキーマの **[概要 (Overview)]** ページに展開の概要が表示されます。

図 6: スキーマの概要



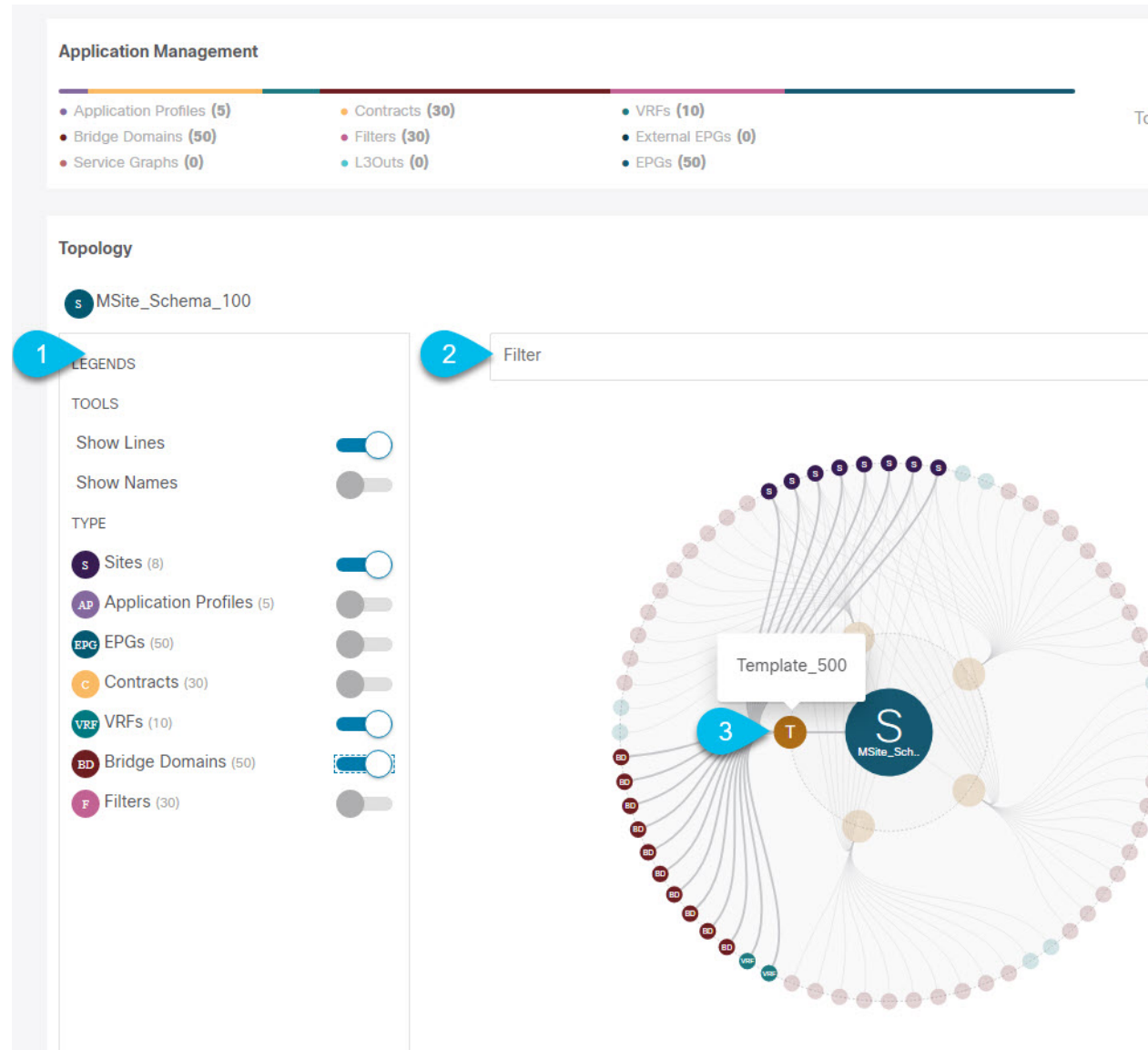
このページには、次の詳細が表示されます。

1. **[一般 (General)]** : 名前や説明など、スキーマの一般情報を提供します。
2. **[監査ログ (Audit Log)]** : スキーマで実行されたアクションの監査ログの概要を提供します。
3. **[サイト (Sites)] > [正常性 (Health)]** : サイトの正常性ステータスでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
4. **[サイト (Sites)] > [タイプ (Type)]** : サイトのタイプでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
5. **[テンプレートとサイトの関連付け (Template to Site Associations)] > [展開ステータス (Deployment Status)]** : 1つ以上のサイトに関連付けられているこのスキーマ内のテンプレートの数とその展開ステータスを提供します。
6. **[テンプレートとサイトの関連付けの整合性 (Template to Site Associations Consistency)]** : 展開されたテンプレートで実行された整合性チェックの数とそのステータスを提供します。 >

7. [アプリケーション管理 (Application Management)] : このスキーマのテンプレートに含まれる個々のオブジェクトの概要を提供します。

[トポロジ (Topology)] タイルでは、次の図に示すように、1 つ以上のオブジェクトを選択してダイアグラムに表示することで、トポロジ ビジュアライザを作成できます。

図 7: 展開ビジュアライザ



1. 凡例 (Legend) : 次のトポロジ図に表示するポリシーオブジェクトを選択できます。
2. [フィルタ (Filter)] : 表示されるオブジェクトを名前に基づいてフィルタリングできます。
3. [トポロジ図 (Topology Diagram)] : サイトに割り当てられているすべてのスキーマ テンプレートで設定されたポリシーを視覚的に表示します。

上記の [設定オプション (Configuration Options)] を使用して、表示するオブジェクトを選択できます。

また、オブジェクトの上にマウスを置くと、すべての依存関係を強調表示できます。

最後に、図内の任意のオブジェクトをクリックすると、他のオブジェクトとの関係だけが表示されます。たとえば、テンプレートをクリックすると、その特定のテンプレート内のすべてのオブジェクトのみが表示されます。

シャドウオブジェクト

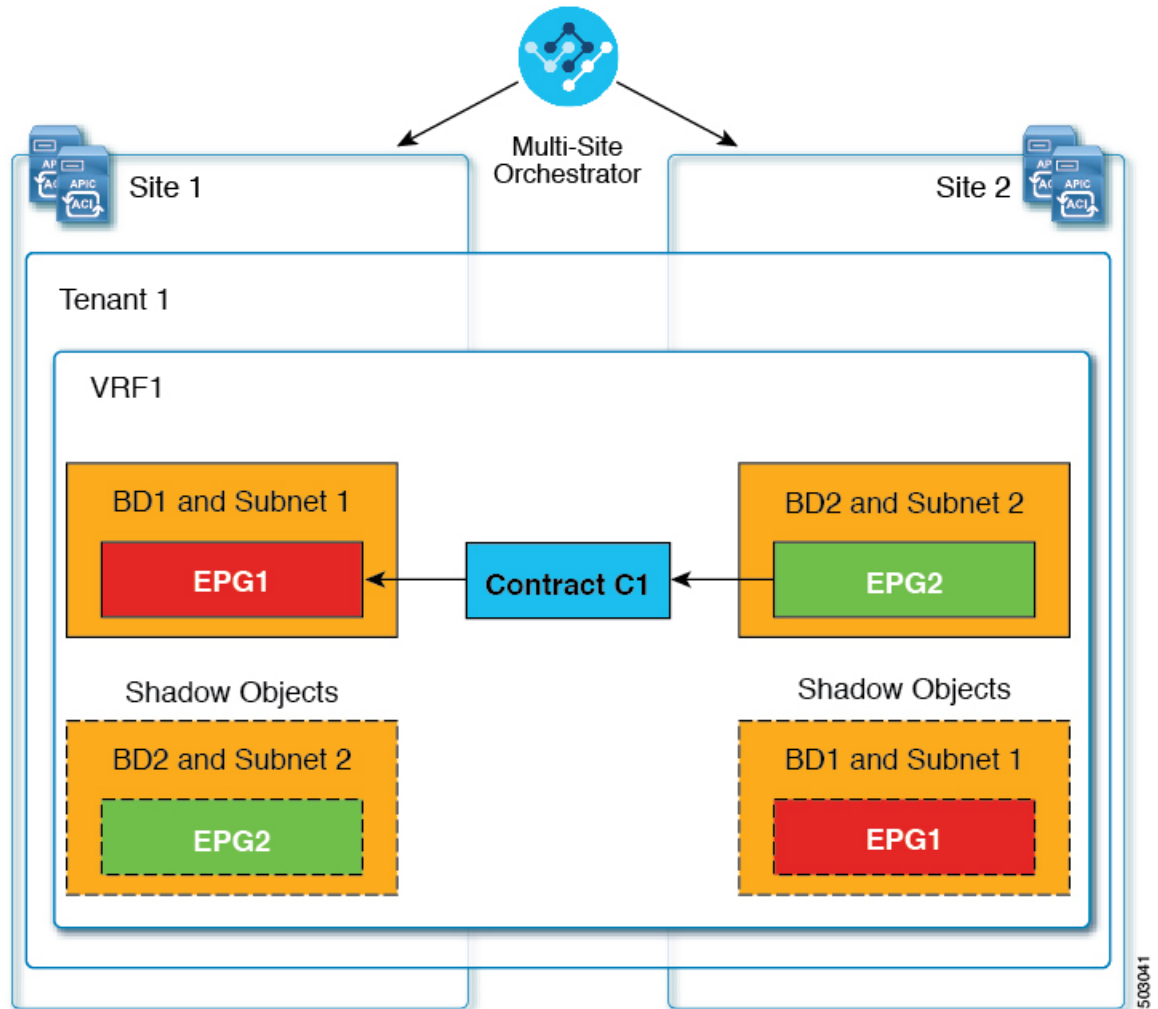
プロバイダとコンシューマーが異なる VRF にあり、テナント コントラクトを介して通信する拡張 VRF または共有サービスの使用例で、サイト ローカル EPG 間にコントラクトが存在する場合、EPG とブリッジドメイン (BD) はリモートサイトにミラーリングされます。ミラーされたオブジェクトは、これらのサイトのそれぞれの APIC で展開されているかのように表示される一方で、実際にはサイトの 1 つでだけ展開されています。これらのミラーされたオブジェクトは、「シャドウ」オブジェクトと呼ばれます。



(注) シャドウ オブジェクトは、APIC GUI を使用して削除する必要があります。

たとえば、テナントと VRF が Site1 と Site2 の間でストレッチされ、プロバイダ EPG とそのブリッジドメインが Site2 のみに展開され、コンシューマ EPG とそのドメインが Site1 のみに展開される場合、対応するシャドウブリッジドメインと EPG は次の図のように展開されます。これらは、直接展開されている各サイトでの名前と同じ名前が表示されます。

図 8: 基本的なシャドウ EPG



次のオブジェクトはシャドウ オブジェクトになる場合があります。

- VRF
- ブリッジ ドメイン (BD)
- L3Out
- 外部 EPG
- アプリケーション プロファイル
- アプリケーション EPG
- コントラクト (ハイブリッドクラウド展開)

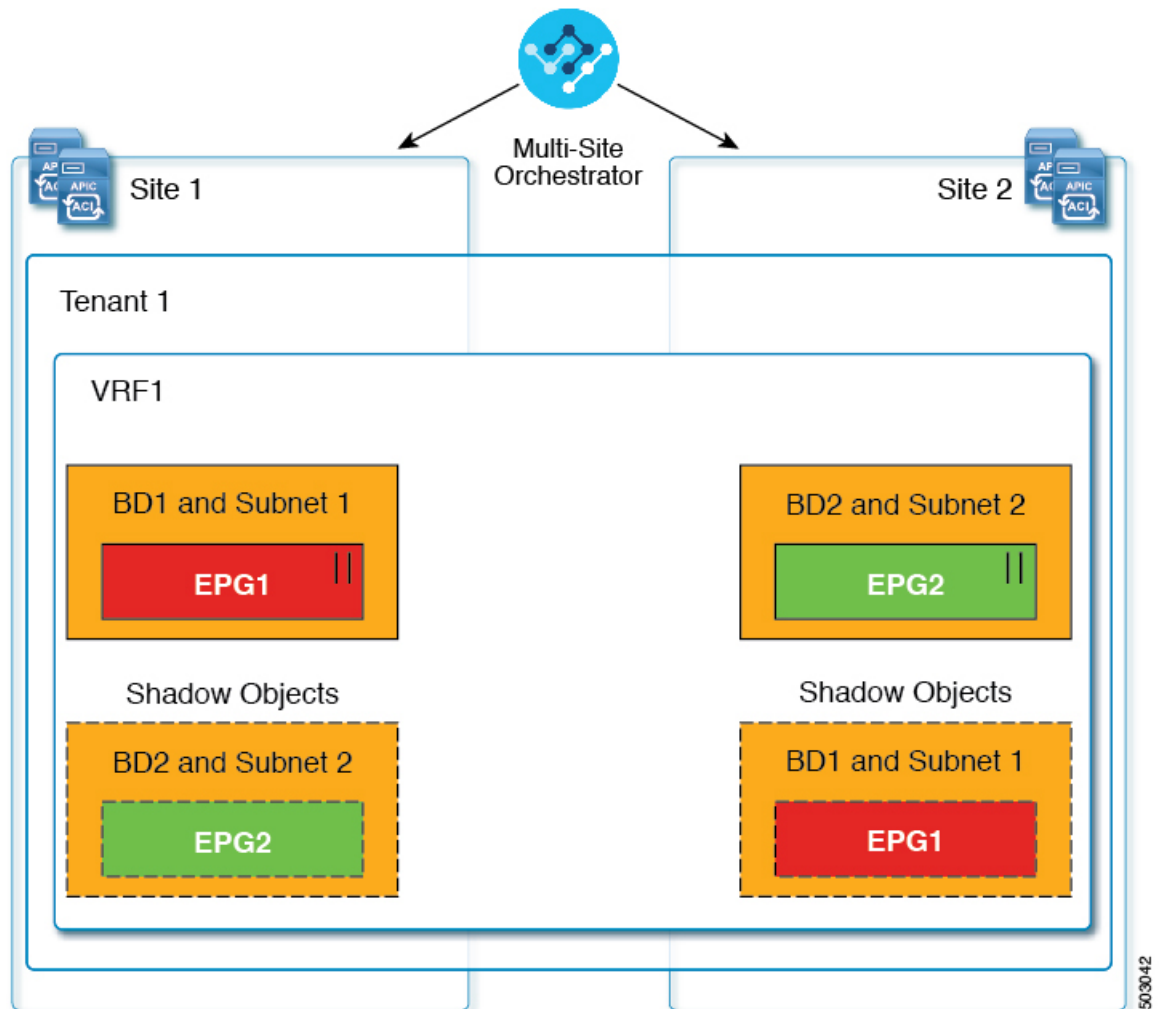
ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュ

されたシャドウ オブジェクトです。このオブジェクトを変更または削除しないでください。メイン GUI ペイン上部の警告。さらに、VMM ドメインの一部ではないシャドウ EPG にはスタティック ポートがないいぼで、シャドウ BD は、APIC GUI で[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]のオプションがあります。

シャドウ オブジェクトのその他の使用例

シャドウ オブジェクトは、次の図に示すように、[優先グループ (Preferred Group)]、[vzAny]、[レイヤ3マルチキャスト (Layer 3 Multicast)]、およびハイブリッドクラウドなど、さまざまな使用例でも作成されます。

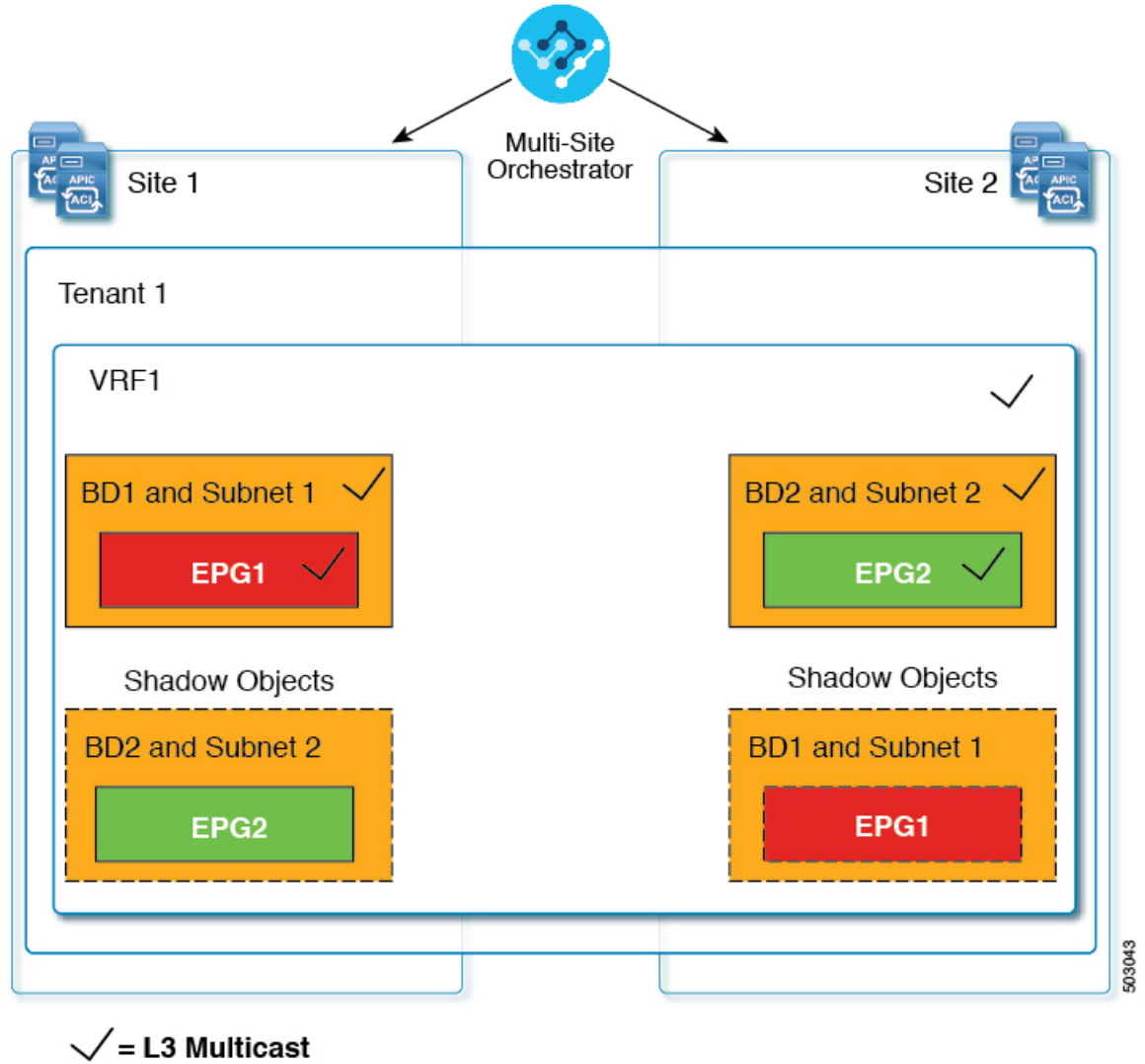
図 9: 優先グループ



|| = Preferred Group

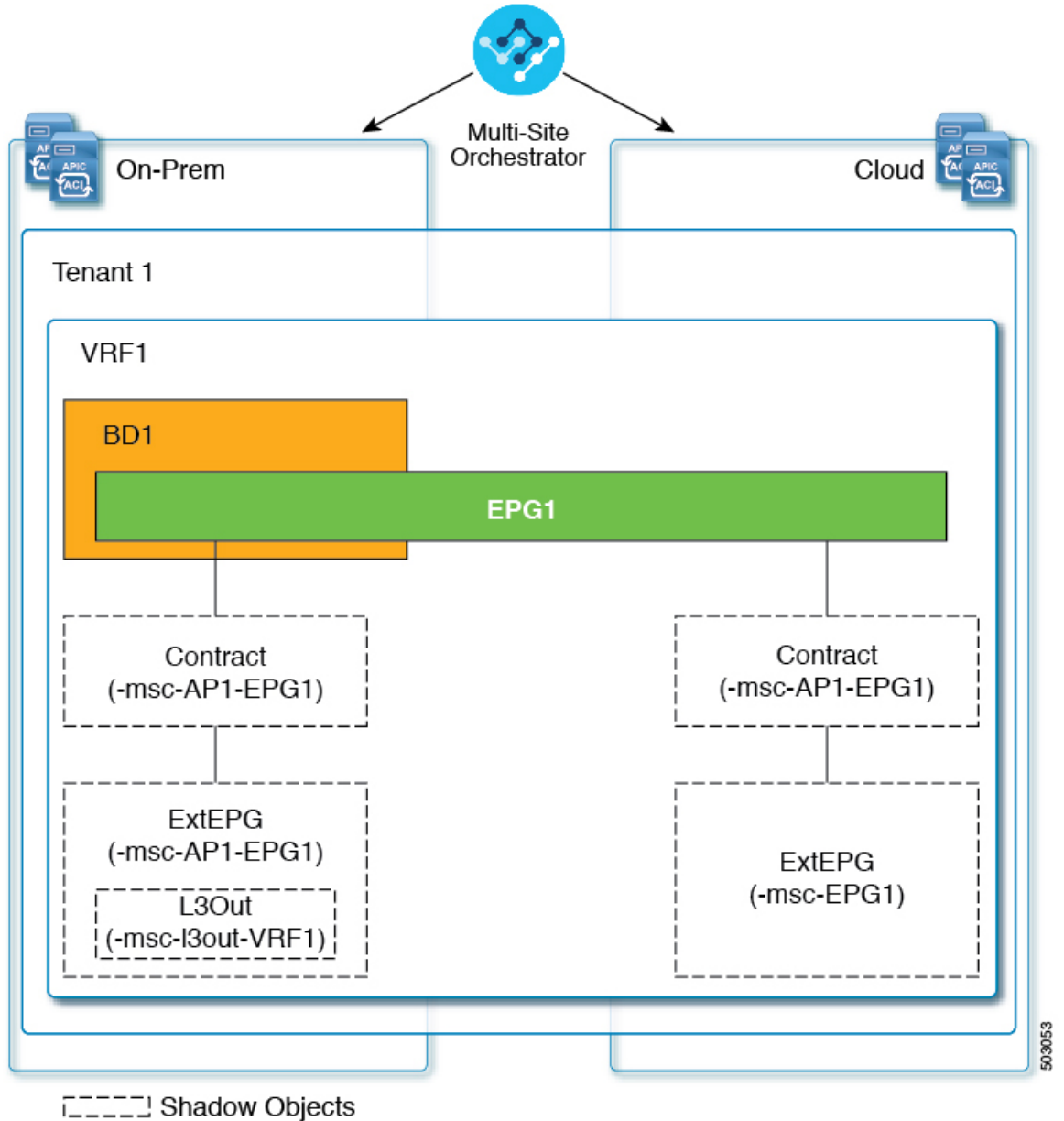
マルチキャストの場合、シャドウ オブジェクトは、マルチキャスト ソースが接続され、オプションが EPG レベルで明示的に設定されている EPG/BD に対してのみ作成されます。

図 10: L3 マルチキャスト



ハイブリッドクラウド展開の場合、ストレッチされたオブジェクトであっても、暗黙のコントラクトが存在するシャドウ オブジェクトを作成します。たとえば、EPG がオンプレミス サイトとクラウドサイトの間でストレッチされた場合、シャドウ外部 EPG は各サイトで作成され、ストレッチされた EPG とシャドウ外部 EPG の間に暗黙的なシャドウ コントラクトが作成されます。

図 11: ハイブリッドクラウド



Cisco APIC リリース 5.2(3) 以降、シャドウ オブジェクトは Cisco APIC GUI で一意のアイコンで示されます。通常の Orchestrator で作成されたオブジェクトは緑のクラウドの記号で表示されますが、シャドウ オブジェクトはグレーのクラウドのアイコンで表示されます。

APIC GUI でシャドウ オブジェクトを非表示にする

APIC リリース 5.0(2) 以降では、オンプレミスサイトの APIC GUI で Nexus Dashboard Orchestrator によって作成されたシャドウ オブジェクトを表示するか非表示にするかを選択できます。Cloud APIC のシャドウ オブジェクトは常に非表示です。

GUI からシャドウ オブジェクトを非表示にするには、次の点に注意してください。

- このオプションは、Orchestrator からグローバルに設定することはできません。また、このセクションで説明するように、各サイトの APIC で直接設定する必要があります。
- シャドウ オブジェクトを表示するオプションはすべての新しい APIC リリース 5.0(2) のインストールとアップグレードのデフォルトでオフに設定されているため、以前に表示されていたオブジェクトが非表示になる可能性があります。
- シャドウ オブジェクトの非表示は、Orchestrator リリース 3.0(2) 以降で使用可能な、Nexus Dashboard Orchestrator によって設定されるフラグに依存しています。

- シャドウ オブジェクトが以前の Orchestrator バージョンによって展開されている場合は、必要なタグがなく、APIC GUI に常に表示されます。

- Shadow オブジェクトが Orchestrator バージョン 3.0(2) 以降で導入されている場合は、タグが付けられ、APIC GUI 設定を使用して非表示または表示にできます。

- Nexus Dashboard Orchestrator をアップグレードする前に、各ファブリックを APIC リリース 5.0(2) にアップグレードすることをお勧めします。

Nexus Dashboard Orchestrator をリリース 3.0(2) にアップグレードすると、APIC リリース 5.0(2) 以降を実行しているサイトに展開されたオブジェクトは、適切なタグでタグ付けされ、再展開しなくても、APIC GUI を使用して表示または非表示にできます。

ファブリックの APIC の前に Orchestrator をアップグレードする場合、サイトのオブジェクトはタグ付けされず、フラグを設定するためにファブリックをアップグレードした後に設定を手動で再展開する必要があります。

- リリース 5.0(2) よりも前のリリースにファブリックをダウングレードした場合、シャドウ オブジェクトは非表示にならず、APIC GUI に異なるアイコンが表示されることがあります。



ステップ 1 サイトの APIC にログインします。

ステップ 2 右上隅にある [マイ プロファイルの管理 (Manage my profile)] アイコンをクリックし、[設定 (Settings)] を選択します。

ステップ 3 [アプリケーション設定 (Application Settings)] ウィンドウで、[非表示のポリシーを表示 (Show Hidden Policies)] チェックボックスをオンまたはオフにします。

この設定はユーザ プロファイルに保存され、ユーザごとに個別に有効または無効になります。

ステップ 4 その他の APIC サイトについては、このプロセスを繰り返します。



第 II 部

操作

- [監査ログ \(87 ページ\)](#)
- [バックアップと復元 \(89 ページ\)](#)
- [サイトのアップグレード \(103 ページ\)](#)
- [テクニカル サポート \(115 ページ\)](#)



第 5 章

監査ログ

- [監査ログ \(87 ページ\)](#)

監査ログ

Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

GUI 内で直接 Nexus Dashboard Orchestrator のログを表示するには、メインのナビゲーションメニューから **[操作 (Operations)]** > **[監査ログ (Audit logs)]** を選択します。

[監査ログ (Audit Logs)] ページで、最新のフィールドをクリックして、ログを表示する特定の期間を選択できます。たとえば、2017 年 11 月 14日から 2017 年 11 月 17日までの範囲を選択し、**[適用 (Apply)]** をクリックすると、この期間の監査ログの詳細が **[監査ログ (Audit Logs)]** ページに表示されます。

次の基準に従ってログの詳細のフィルタ処理を行うには、**[フィルタ (Filter)]** アイコンをクリックします。

- **ユーザ (User)**: ユーザタイプに基づいて監査ログのフィルタ処理を行うには、このオプションを選択し、**[適用 (Apply)]** をクリックします。
- **タイプ (Type)**: 監査ログをポリシータイプ (サイト、ユーザ、テンプレートなど) でフィルタリングするには、このオプションを選択して、**[適用 (Apply)]** をクリックします。
- **アクション (Action)**: アクションに基づいて監査ログをフィルタ処理するには、このオプションを選択します。使用可能なアクションとしては作成、更新、削除、追加、関連付け、関連付けの解除解除、展開、展開の解除、ダウンロード、アップロード、復元、ログイン、ログの失敗があります。アクションに従ってログの詳細をフィルタ処理するには、アクションを選択して **Apply** をクリックします。



第 6 章

バックアップと復元

- 設定のバックアップと復元 (89 ページ)
- バックアップと復元に関するガイドライン (89 ページ)
- バックアップのリモート ロケーションの設定 (93 ページ)
- バックアップのアップロード (94 ページ)
- バックアップの作成 (95 ページ)
- バックアップの復元 (96 ページ)
- バックアップのダウンロード (100 ページ)
- バックアップ スケジューラ (101 ページ)

設定のバックアップと復元

Nexus Dashboard Orchestrator の障害またはクラスタの再起動からのリカバリを容易にする、Orchestrator 設定のバックアップを作成できます。Orchestrator の各アップグレードまたはダウングレードの前で、各設定の変更または展開後に、設定のバックアップを作成することを推奨します。バックアップは常に、Nexus Dashboard Orchestrator で定義されているリモート サーバ (Nexus Dashboard クラスタ以外) に作成されます。定義については、続くセクションで説明します。

バックアップと復元に関するガイドライン

設定のバックアップを保存および復元する際には、次のガイドラインが適用されます。

- より新しいリリースから作成されたバックアップのインポートおよび復元はサポートされていません。

たとえば、Nexus Dashboard Orchestrator を以前のリリースにダウングレードした場合、それ以降のリリースで作成された設定のバックアップを復元することはできません。

- リリース 3.2(1) より前のリリースで作成された設定バックアップの復元は、Nexus Dashboard へのクラスタ移行中のワンタイム ステップとしてサポートされます。

VMware ESX または Application Services Engine 展開で、Multi-Site Orchestrator リリースからバックアップしていた場合、その後の復元はサポートされていません。

クラスタを Nexus ダッシュボードに移行する詳細な手順については、『[Cisco Nexus Dashboard Orchestrator 展開ガイド](#)』の「既存のクラスタから Nexus ダッシュボードへの移行」の章を参照してください。

- バックアップを保存すると、設定は展開されたのと同じ状態で保存されます。バックアップを復元すると、展開されたすべてのポリシーが展開済みとして表示されますが、展開されていなかったポリシーは未展開の状態のままになります。
- バックアップアクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ（APIC、Cloud APIC、NDFC/DCNM など）データベースは変更されません。

Orchestrator データベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示されている構成のばらつきがある場合はそれらを解決してから、既存のテンプレートを再展開して、Nexus Dashboard Orchestrator と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。

- バックアップはリモート ロケーションで作成する必要があります。

リリース 3.4(1) よりも前のリリースでは、クラスタを最初に展開したとき、作成していたバックアップは、各ノードのローカルディスク上のデフォルトの場所に保存され、さらに Orchestrator クラスタ外のリモート ロケーションを設定して、そこにバックアップを再配置するオプションがありました。

リリース 3.4(1) 以降では、ローカルディスク オプションは廃止されたので、すべてのバックアップは Nexus ダッシュボード クラスタ外のリモート ロケーションに作成する必要があります。次のセクションの説明に従って、NDO GUI を使用してリモート SCP または SFTP ロケーションを設定し、そこにバックアップ ファイルをエクスポートできます。

リリース 3.3(1) 以前からリリース 3.4(1) 以降に初めてアップグレードする場合は、[古いローカルバックアップのダウンロードとインポート \(92 ページ\)](#) の説明に従って、以前に作成したローカルバックアップをダウンロードできます。その後、リモートロケーションを経由して、これらのバックアップを Nexus Dashboard Orchestrator に再インポートできます。



(注) ローカルバックアップは復元できません。

- 設定のバックアップを作成してリモートサーバにエクスポートするときには、ファイルは最初に Orchestrators ローカルドライブに作成され、その後リモートの場所にアップロードされ、最後にローカルストレージから削除されます。十分なローカルディスク領域がない場合、バックアップは失敗します。
- リリース 3.4(1) 以降にアップグレードする前に、ローカルバックアップを取得できるようにバックアップスケジューラを有効にしていた場合、アップグレード後に無効になります。

バックアップ以降の設定変更はありません

バックアップが作成されてから復元されるまでの間にポリシーの変更がない場合は、追加の考慮事項は必要ありません。また、[バックアップの復元 \(96 ページ\)](#) の説明に従って設定を復元するだけです。

バックアップ以降に作成、変更、または削除されたサイト、オブジェクトまたはポリシー

設定のバックアップが作成されてから復元された時間までの間に設定変更が行われた場合は、次の点を考慮してください。

- バックアップを復元しても、サイトのオブジェクト、ポリシー設定は変更されません。バックアップ以降に作成および展開された新しいオブジェクトまたはポリシーは、展開されたままになります。

Orchestrator データベースを復元した後、このガイドの「構成のbaratukiドリフト」セクションで説明されているように、テンプレートに表示される可能性のある構成のドリフトを解決してから、既存のテンプレートを再デプロイして、Nexusダッシュボード間でポリシーが一致しない可能性を回避することをお勧めします。オーケストレーターと各サイトのコントローラー。We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

または、すべてのポリシーを最初に展開解除することもできます。これにより、バックアップから設定が復元された後に、古いオブジェクトの潜在的な問題が回避されます。ただし、これにより、これらのポリシーによって定義されたトラフィックまたはサービスの中断が発生します。

- 設定のバックアップを復元するために必要な手順については、[バックアップの復元 \(96 ページ\)](#) で説明しています。
- 復元した設定バックアップが、サイトに展開される前に保存されたものであった場合、未展開状態で復元されるので、必要に応じてサイトに展開できます。
- 復元した設定バックアップが、設定がすでに展開されているときに保存されたものであった場合、サイトにどの設定もまだ存在していなかったとしても、展開済み状態で復元されません。

この場合、このガイドの「構成のドリフト」セクションで説明されているように、テンプレートに表示されている構成のばらつきがある場合はそれらを解決し、テンプレートを再展開して、Nexus Dashboard Orchestrator の構成をサイトと同期します。

- バックアップの作成時に管理されていたサイトが Nexus ダッシュボードに存在しない場合、復元は失敗します。
- バックアップ後にサイトのステータス（管理対象と非管理対象）を変更していて、サイトが Nexus ダッシュボードにまだ存在している場合、ステータスはバックアップ時の状態に復元されます。

古いローカルバックアップのダウンロードとインポート

3.4(1) より前のリリースでは、オーケストレータのローカルディスクでの設定バックアップの作成がサポートされていました。リリース 3.4(1) 以降にアップグレードする前に、ローカルバックアップをダウンロードしておくことを推奨します。ただし、ローカルバックアップはアップグレード後も引き続きダウンロードできます。

アップグレード後に古いバックアップをダウンロードすることはできますが、UI で直接バックアップを復元することはできません。このセクションでは、このようなバックアップを Orchestrator GUI からローカルマシンにダウンロードし、今度はリモートロケーションを使用して Nexus Dashboard Orchestrator GUI に再インポートする方法について説明します。

始める前に

次の設定が済んでいる必要があります。

- リリース 3.3(1) 以前からリリース 3.4(1) 以降にアップグレードされていること。新しいリリースでは、ローカルバックアップはサポートされなくなりました。
- [バックアップのリモートロケーションの設定 \(93 ページ\)](#) の説明に従って、バックアップのためのリモートロケーションが追加されていること。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションメニューで、**[操作 (Operations)] > [バックアップと復元 (Backups & Restore)]** を選択します。

ステップ 3 メインウィンドウで、ダウンロードするバックアップの隣のアクション (...) アイコンをクリックし、**[ダウンロード (Download)]** を選択します。

これにより、バックアップファイルがシステムにダウンロードされます。

ステップ 4 Nexus Dashboard Orchestrator GUI でダウンロードしたバックアップを削除します。

以前のバージョンから既存のローカルバックアップを削除せずにバックアップを再インポートしようとすると、同じ名前のバックアップファイルがすでに存在するため、アップロードが失敗します。

ダウンロードしたバックアップを削除するには、バックアップの横にあるアクション (...) メニューをクリックし、**[削除 (Delete)]** を選択します。

ステップ 5 バックアップをリモートの場所にインポートします。

[バックアップのアップロード \(94 ページ\)](#) に記載されているように、リモートロケーションを使用してダウンロードしたバックアップファイルを Nexus Dashboard Orchestrator に再アップロードします。

バックアップのリモートロケーションの設定

このセクションでは、設定バックアップをエクスポートできる Nexus Dashboard Orchestrator のリモートロケーションの設定方法を説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションペインで、**[操作 (Operations)] > [リモートロケーション (Remote Location)]** を選択します。

ステップ 3 メインウィンドウの右上隅で、**[リモートロケーションの追加 (Add Remote Location)]** をクリックします。
[新規リモートロケーションの追加 (Add New Remote Location)] 画面が表示されます。

ステップ 4 リモートロケーションの名前と説明 (任意) を入力します。

現在、2つのプロトコルが設定バックアップのリモートエクスポートに対してサポートされています。

- SCP
- ステップ

(注) SCPは Windows 以外のサーバーでのみサポートされます。リモートロケーションが Windows サーバーの場合は、SFTP プロトコルを使用する必要があります。

ステップ 5 リモートサーバーのホスト名または IP アドレスを指定します。

[プロトコル (Protocol)] セクションに基づいて、指定するサーバーでは SCP または SFTP 接続を許可する必要があります。

ステップ 6 バックアップを保証するリモートサーバーのディレクトリにフルパスを指定します。

パスの先頭にはスラッシュ (/) 文字を使用し、ピリオド (.) とバックスラッシュ (\) を含むことはできません。例: `/backups/multisite`

(注) ディレクトリは、リモートサーバーにすでに存在しなければなりません。

ステップ 7 リモートサーバーに接続するために使用するポートを指定します。

デフォルトで、ポートは 22 に設定されます。

ステップ 8 リモートサーバーに接続するときを使用される認証タイプを指定します。

次の2つの認証方式のうちの1つを使用して設定できます。

- パスワード—リモートサーバーにログインするために使用されるユーザ名とパスワードを指定します。
- SSH プライベートファイル—ユーザ名とリモートサーバーにログインするために使用される SSH キー/パスワードのペアを指定します。

ステップ9 [保存 (Save)] を使用して、リモート サーバを追加します。

バックアップのアップロード

ここでは、以前にダウンロードした既存の設定バックアップをアップロードし、Nexus Dashboard Orchestratorで設定されたリモートロケーションのいずれかにインポートする方法について説明します。

始める前に

次の設定が済んでいる必要があります。

- [バックアップの作成 \(95 ページ\)](#) および [バックアップのダウンロード \(100 ページ\)](#) の説明に従って、設定のバックアップを作成されていること。
リリース 3.4(1)以降で作成したバックアップなど、バックアップがすでにリモートロケーションにある場合は、ローカルマシンにダウンロードして、別のリモートロケーションにアップロードできます。
- [バックアップのリモートロケーションの設定 \(93 ページ\)](#) の説明に従って、バックアップのためのリモートロケーションが追加されていること。

ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ2 左側のナビゲーションペインで、[操作 (Operations)] > [バックアップと復元 (Backups & Restore)] を選択します。

ステップ3 メインペインで、[アップロード (Upload)] をクリックします。

ステップ4 開いた [ファイルからのアップロード (Upload from file)] ウィンドウで、[ファイルを選択 (Select File)] を選択して、インポートするバックアップファイルを選択します。

バックアップをアップロードすると、[バックアップ (Backups)] ページに表示されるバックアップのリストに追加されます。

ステップ5 [リモートロケーション (Remote location)] ドロップダウンメニューから、リモートロケーションを選択します。

ステップ6 (オプション) リモートロケーションのパスを更新します。

リモートバックアップのロケーションを作成するときに設定したリモートサーバ上のターゲットディレクトリが、[リモートパス (Remote Path)] フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモートサーバで作成されている必要があります。

ステップ7 [アップロード (Upload)] をクリックしてファイルをインポートします。

バックアップのインポートは、[バックアップ (Backups)] ページに表示されたバックアップのリストにそれを追加します。

バックアップは NDO UI に表示されますが、リモート サーバーにのみ存在することに注意してください。

バックアップの作成

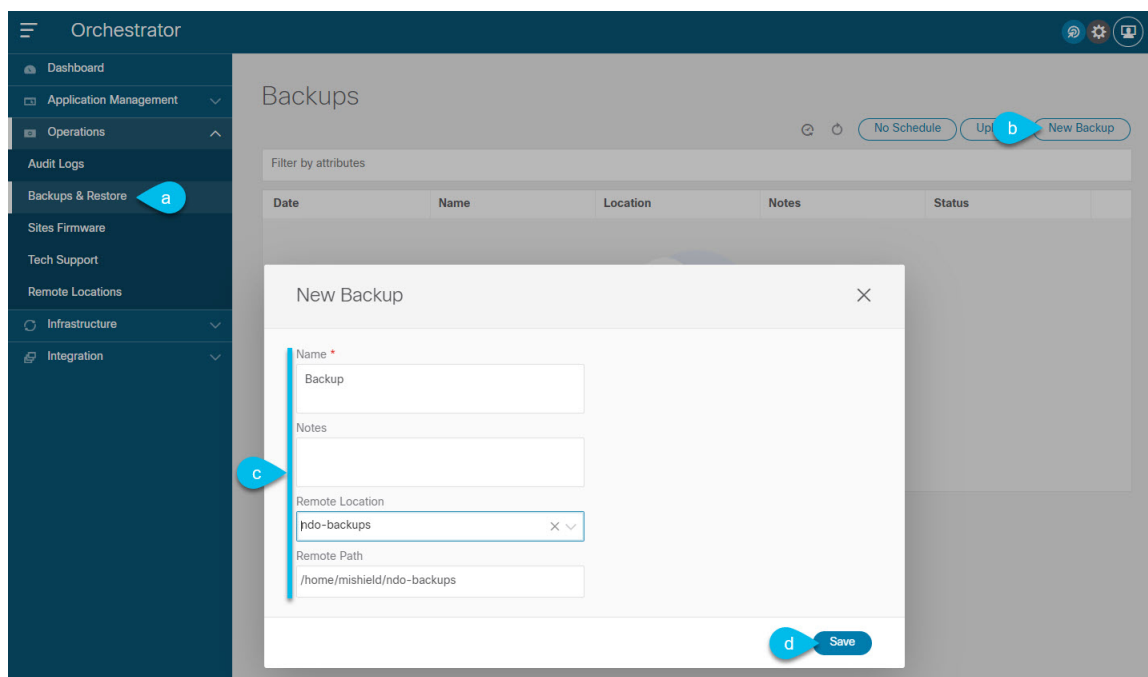
ここでは、Nexus Dashboard Orchestrator 設定の新しいバックアップを作成する方法について説明します。

始める前に

バックアップのリモート ロケーションの設定 (93 ページ) の説明に従って、最初にリモート ロケーションを追加する必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 既存の展開設定をバックアップします。



a) 左側のナビゲーション ペインで、[操作 (Operations)] > [バックアップと復元 (Backups & Restore)] を選択します。

b) メイン ウィンドウ ペインで、[新規バックアップ (New Backup)] をクリックします。

[新規バックアップ (New Backup)] ウィンドウが開きます。

c) バックアップ情報を提供します。

- **[名前 (Name)]** フィールドに、バックアップ ファイルの名前を入力します。
名前には、最大 10 文字の英数字を使用できますが、スペースまたはアンダースコア () は使用できません。
- **[リモートロケーション (Remote location)]** ドロップダウンから、バックアップを保存するために構成したリモートロケーションを選択します。
- (オプション) **[リモートパス (Remote Path)]** では、バックアップを保存する先のリモートサーバーの特定のディレクトリを提供します。
指定するディレクトリはすでに存在する必要があります。

d) **[保存 (Save)]** をクリックして、バックアップを作成します。

バックアップの復元

このセクションでは、Orchestrator 設定を前の状態に復元する方法について説明します。

始める前に

- 「[バックアップのリモートロケーションの設定 \(93 ページ\)](#)」で説明されているように、NDO バックアップを保存するためのリモートロケーションを構成しておく必要があります。
- 「[バックアップのアップロード \(94 ページ\)](#)」の説明に従って、復元するバックアップがリモートロケーションサーバーにあることを確認するか、バックアップをリモートロケーションにインポートします。



(注) バックアップアクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ (APIC、Cloud APIC、NDFC/DCNM など) データベースは変更されません。

Orchestrator データベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示されている構成のばらつきがある場合はそれらを解決してから、既存のテンプレートを再展開して、Nexus Dashboard Orchestrator と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。

特定の構成の不一致とそれぞれに関連する望ましい復元手順の詳細は、[バックアップと復元に関するガイドライン \(89 ページ\)](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 必要に応じて、既存のポリシーの展開を解除します。

バックアップが作成されたときから現在の設定までに、設定に新しいオブジェクトまたはポリシーが追加されている場合は、この手順を実行することをお勧めします。追加情報については、[バックアップと復元に関するガイドライン \(89 ページ\)](#) を参照してください。

ステップ 3 左側のナビゲーションメニューで、**[操作 (Operations)] > [バックアップと復元 (Backups & Restore)]** を選択します。

ステップ 4 メインウィンドウで、復元するバックアップの隣のアクション(...) アイコンをクリックし、**[このバックアップにロールバック (Rollback to this backup)]** を選択します。

選択したバックアップのバージョンが、実行中の Nexus Dashboard Orchestrator のバージョンと異なる場合、ロールバックが原因で、バックアップされたバージョンには存在しない機能が削除される可能性があります。

ステップ 5 **[はい (Yes)]** をクリックして、選択したバックアップを復元することを確認します。

[はい (Yes)] をクリックすると、システムは現在のセッションを終了して、ユーザはログアウトされます。

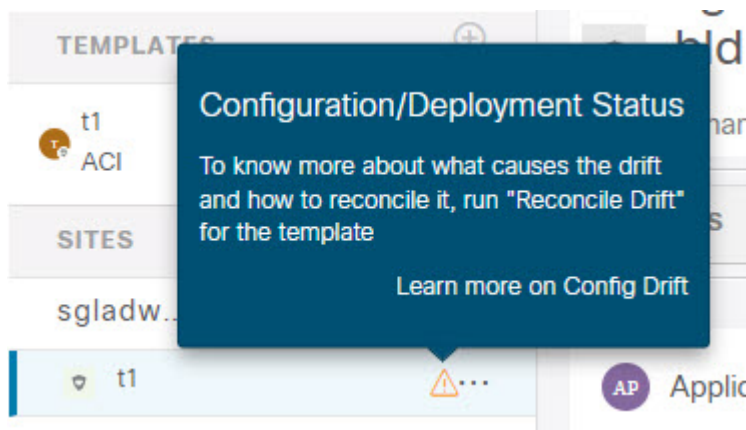
(注) 設定の復元プロセス中に複数のサービスが再起動されます。その結果、復元された設定が NDO GUI に正しく反映されるまでに最大 10 分の遅延が発生することがあります。

ステップ 6 構成のばらつきがあるかどうか、すべてのテンプレートを確認してください。

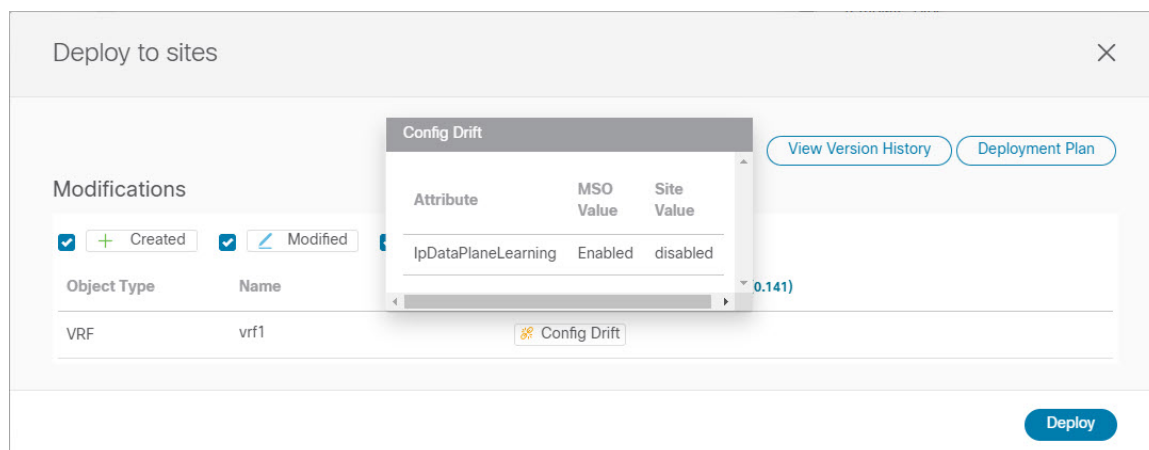
展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきを確認できます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータスアイコンを確認します。



- テンプレートを選択し、**[サイトへの展開 (Deploy to sites)]** をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。



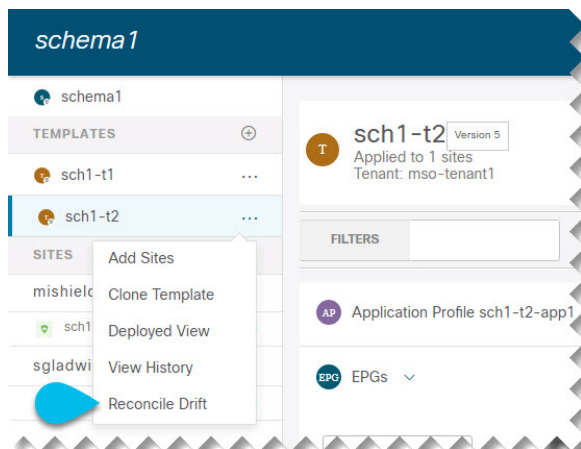
ステップ 1 構成のばらつきが含まれているテンプレートがある場合は、競合を解決します。

構成のばらつきの詳細については、『[Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics](#)』の「構成のばらつき」の詳細を確認してください。

- a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

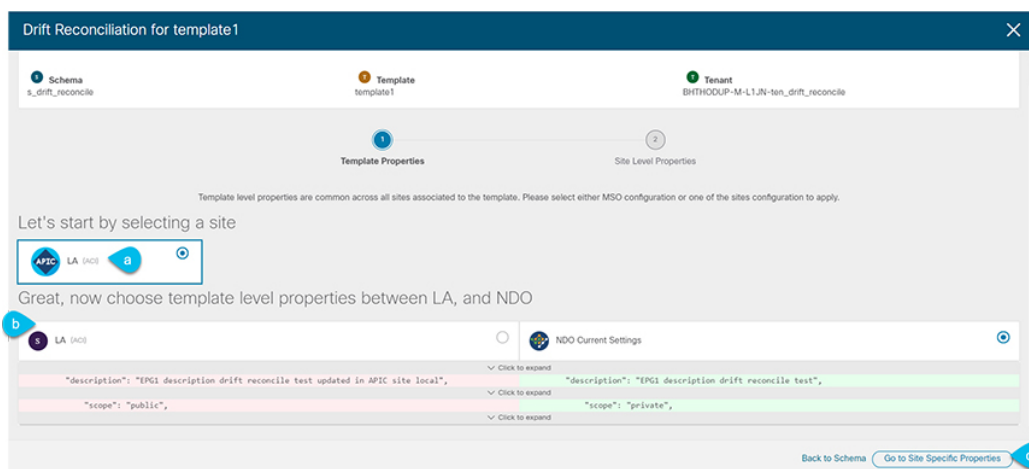
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

- b) テンプレートの [アクション (Actions)] メニューから、[ばらつきの調整 (Reconcile Drift)] を選択します。



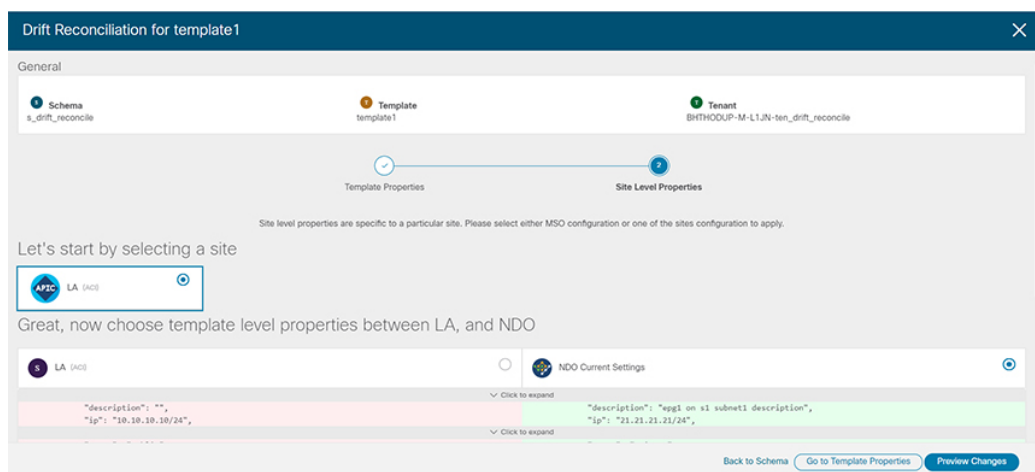
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

- c) [ばらつきの調整 (Reconcile Drift)] 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレートレベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変更されますが、Nexus Dashboard Orchestrator 構成を選択した場合は、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま保持されます。

- d) [**サイト固有のプロパティに移動 (Go to Site Specific Properties)**] をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカルプロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルの構成とサイトレベルの構成のどちらでも同じ選択を行います。ばらつきの調整ウィザードでは、サイトのコントローラで定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

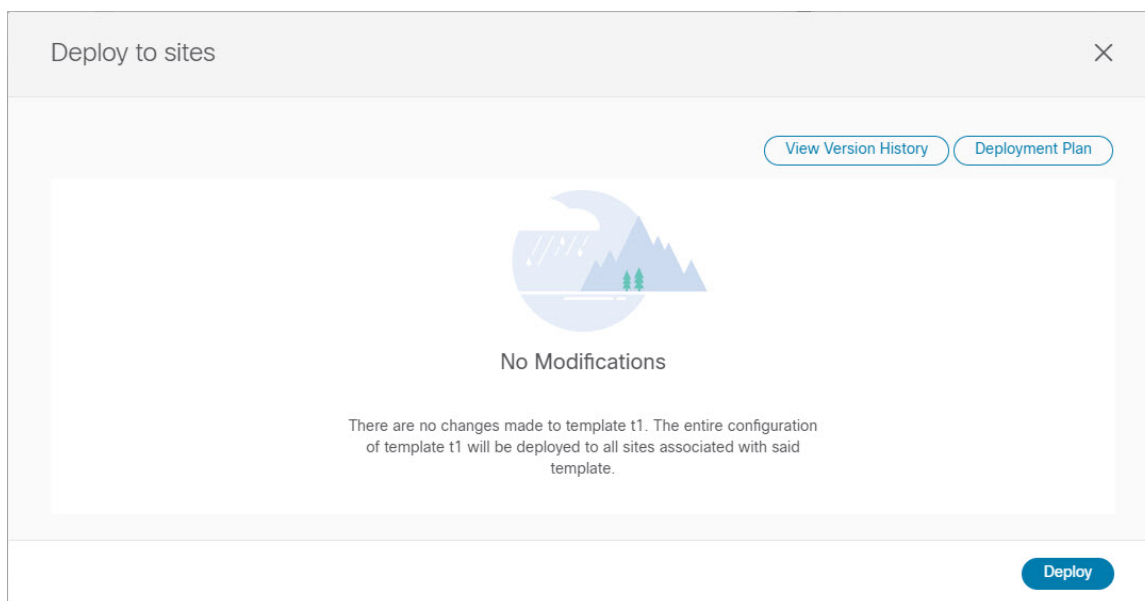
- e) [**変更のプレビュー (Preview Changes)**] をクリックして、選択内容を確認します。

プレビューは[ばらつきの調整 (Reconcile Drift)] ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、[サイトに展開 (Deploy to site)] をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

ステップ 8 すべての構成のばらつきが解決され、[サイトへの展開 (Deploy to sites)] ダイアログに変更が表示されなくなったら、テンプレートの完全な再展開を実行します。

(注) リリース 3.7(1) のデータベース変換のため、各テンプレートの完全な再展開を実行する必要があります。

次の図に示すように、[サイトへの展開 (Deploy to sites)] ダイアログに変更が含まれていないことを確認し、[展開 (Deploy)] をクリックして、完全な構成を再展開します。



ステップ 9 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 10 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション (Operations)] タブの監査ログを表示できます。

[監査ログ (Audit Logs)] ページで、すべてのテンプレートが [再展開済み (Redeployed)] と表示され、完全な再展開が正常に完了したことを確認します。

バックアップのダウンロード

ここでは、Nexus Dashboard Orchestrator からバックアップをダウンロードする方法について説明します。

始める前に

- ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ2 左側のナビゲーションメニューで、[操作 (Operations)] > [バックアップと復元 (Backups & Restore)] を選択します。
- ステップ3 メインウィンドウで、ダウンロードするバックアップの隣のアクション(...) アイコンをクリックし、[ダウンロード (Download)] を選択します。

これにより `msc-backups-<タイムスタンプ>.tar.gz` 形式でシステムにバックアップファイルがダウンロードされます。その後、ファイルを抽出してその内容を表示することができます。

バックアップスケジューラ

ここでは、定期的に完全な設定バックアップを実行するバックアップスケジューラを有効または無効にする方法について説明します。

始める前に

[バックアップのリモートロケーションの設定 \(93 ページ\)](#) の説明に従って、バックアップのためのリモートロケーションを追加してある必要があります。

- ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ2 左側のナビゲーションメニューで、[操作 (Operations)] > [バックアップと復元 (Backups & Restore)] を選択します。
- ステップ3 メインペインの右上にある [スケジューラ (Scheduler)] をクリックします。
[バックアップスケジューラ設定 (Backup Scheduler Settings)] ウィンドウが開きます。
- ステップ4 バックアップスケジューラをセットアップします。
 - a) [スケジューラの有効化 (Enable Scheduler)] チェックボックスをオンにします。
 - b) [開始日の選択 (Select Start Date)] フィールドに、スケジューラを開始する日を指定します。
 - c) [時間の選択 (Select Time)] フィールドに、スケジューラを開始する時刻を入力します。
 - d) [頻度の選択 (Select Frequency)] ドロップダウンから、バックアップを実行する頻度を選択します。
 - e) [リモートロケーション (Remote Location)] ドロップダウンから、バックアップを保存する場所を選択します。
 - f) (オプション) [リモートパス (Remote Path)] フィールドで、バックアップが保存されるリモートロケーションのパスを更新します。

リモートバックアップのロケーションを作成するときに設定したリモートサーバ上のターゲットディレクトリが、[リモートパス (Remote Path)] フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモートサーバで作成されている必要があります。

g) [OK] をクリックして終了します。

ステップ 5 バックアップスケジューラを無効にする場合は、上記の手順で[スケジューラの有効化 (Enable Scheduler)] チェックボックスをオフにします。



第 7 章

サイトのアップグレード

- 概要 (103 ページ)
- 注意事項と制約事項 (105 ページ)
- コントローラとスイッチノードのファームウェアをサイトにダウンロードする (106 ページ)
- コントローラのアップグレード (108 ページ)
- ノードのアップグレード (110 ページ)

概要



(注) この機能は、Cisco APIC サイトでのみサポートされます。Cisco Cloud APIC または Cisco DCNM ファブリックではサポートされません。

リリース 3.1(1) よりも前は、Cisco Multi-Site を導入する際に、各サイトの APIC クラスタおよびスイッチノードソフトウェアをサイトレベルで個別に管理する必要がありました。Multi-Site ドメイン内のサイトの数が増えると、リリースのライフサイクルとアップグレードは、リリースと機能の互換性のために手動で調整および管理する必要があるため、複雑になる可能性があります。

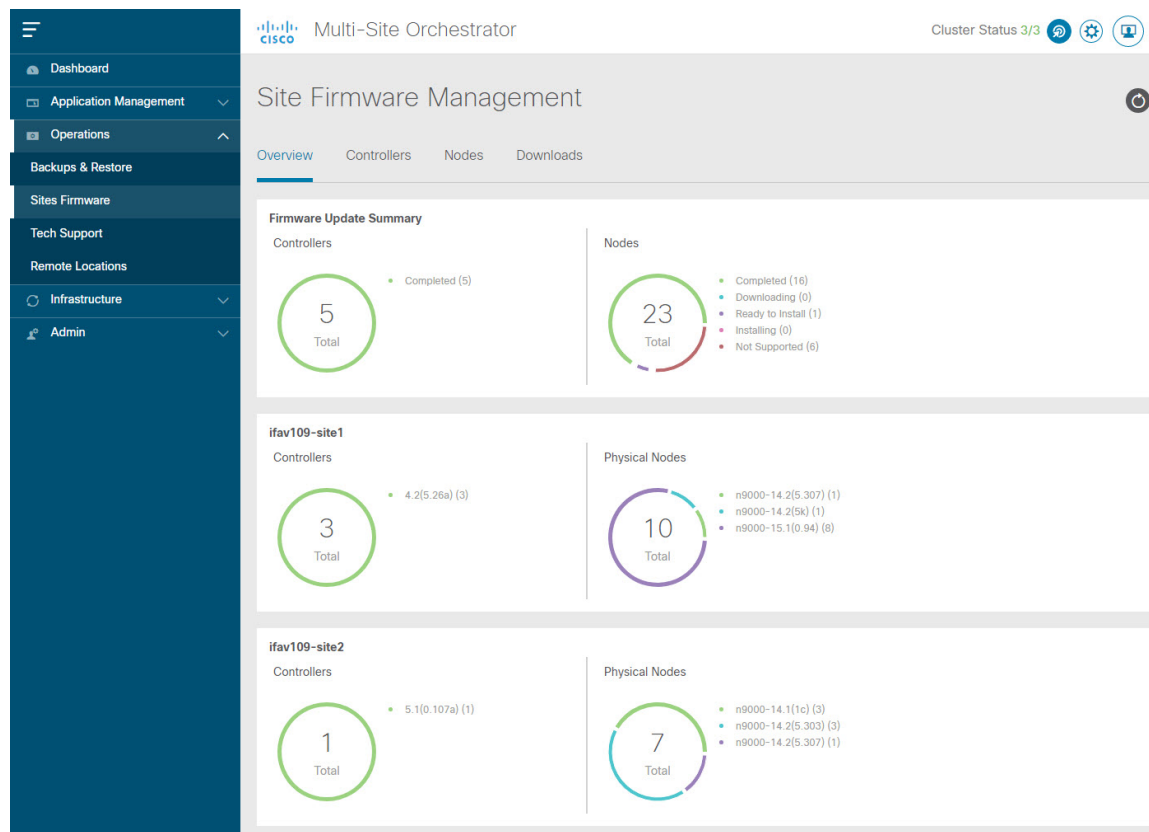
リリース 3.1(1) 以降、Cisco Nexus Dashboard Orchestrator は、すべてのサイトのソフトウェアアップグレードを単一のポイントから管理できるワークフローを提供します。複数のサイト管理者がソフトウェアアップグレードを手動で調整する必要がなく、アップグレードに影響する可能性のある、潜在的な問題を把握できます。

[操作 (Operations)] > [サイトのファームウェア (Sites Firmware)] に移動して、サイトのアップグレード画面にアクセスできます。このページには4つのタブがあります。このセクションと次のセクションで説明します。

[概要 (Overview)] タブには、Multi-Site ドメイン内のサイトと、展開されている、または展開の準備ができていないファームウェアバージョンに関する情報が表示されます。[サイト ファームウェア (Sites Firmware)] サービスは、5分ごとにサイトをポーリングして、アップグレードポリシーの最新のステータスなどの新しいデータまたは変更されたデータを探します。メイン

ページの右上隅にある **[更新 (Refresh)]** ボタンをクリックすると、手動で更新をトリガーできます。

図 12: サイトのファームウェアの概要



ページは次の 3 つの領域に分かれています。

- **[ファームウェア アップデートの概要 (Firmware Update Summary)]** : Cisco APICおよびスイッチ ファームウェアを含む、Multi-Site ドメイン内のすべてのサイトに存在するファームウェア イメージの全体的な概要を提供します。

イメージのタイプごとに、各状態のイメージ数を含む、固有の情報が表示されます。

- [完了 (Completed)] : イメージは現在、コントローラまたはスイッチに展開されています。
- [ダウンロード中 (Downloading)] (スイッチノードのみ) : イメージはスイッチ ノードにダウンロード中です。
- [インストールの準備完了 (Ready to Install)] (スイッチノードのみ) : イメージはスイッチノードに正常にダウンロードされ、インストールの準備ができています。
- [インストール (Installing)] : コントローラまたはスイッチノードに現在イメージを展開中です。

- [未サポート (Not Supported)] : リリース 4.2(5) より前のリリースなど、リモートファームウェア アップグレードをサポートしていないイメージ。
- [サイト固有の情報 (Site-specific information)] : ページの追加のセクションには、個々のサイトに関する情報が表示されます。これには、現在展開されているソフトウェアのバージョンと、コントローラまたはノードの数が含まれます。

注意事項と制約事項

Nexus Dashboard Orchestrator からファブリック アップグレードを実行する場合、次の制限が適用されます。

- 「[Upgrade and Downgrading the Cisco APIC and Switch Software](#)」 (『[Cisco APIC Installation, Upgrade, and Downgrade Guide](#)』) に記載されている Cisco APIC アップグレードプロセスに固有のガイドライン、推奨事項、および制限事項を確認し、それに従う必要があります。
- Nexus Dashboard Orchestrator を Cisco Nexus Dashboard に展開する必要があります。

サイトのアップグレード機能は、VMware ESXのNDO導入では使用できません。また、『[Cisco APIC Installation, Upgrade, and Downgrade Guide](#)』に記載されている標準のアップグレード手順に従う必要があります。

- ファブリックは、Cisco APIC リリース 4.2(5) 以降を実行している必要があります。
以前の APIC リリースを実行しているファブリックは、アップグレードワークフロー中に選択できません。『[Cisco APIC Installation, Upgrade, and Downgrade Guide](#)』に記載されている標準のアップグレード手順に従います。
- サイトのアップグレードは、これらのファブリックを管理するサイト管理者と調整することを推奨します。潜在的な問題が発生した場合は、トラブルシューティングのためにコントローラまたはスイッチ ノードにアクセスする必要があります。
- アップグレードプロセスの途中でファブリック スイッチ ノードが非アクティブ状態になった場合 (たとえば、ハードウェアまたは電源障害) 、プロセスは完了できません。この間、ノードアップグレード ポリシーを削除または変更することはできません。これは、NDO がノードがダウンしたか、または単にアップグレードのリポート中かを区別できないためです。

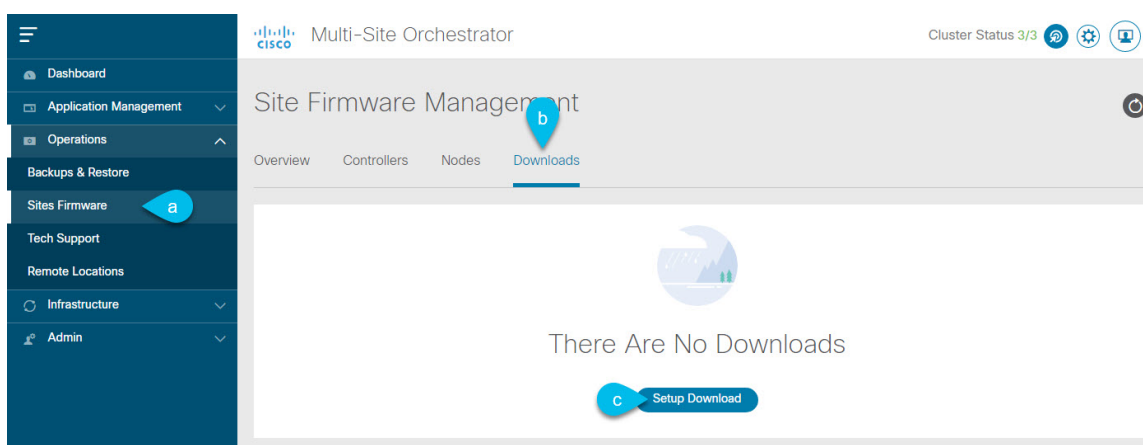
この問題を解決するには、非アクティブノードを APIC から手動でデコミッションする必要があります。この時点で、NDO アップグレードポリシーは変更を認識し、失敗ステータスを返します。その後、NDO のアップグレード ポリシーを更新してスイッチを削除し、アップグレードを再実行できます。

コントローラとスイッチノードのファームウェアをサイトにダウンロードする

アップグレードを実行する前に、コントローラとスイッチソフトウェアをファブリック内のすべてのサイトコントローラにダウンロードする必要があります。次の手順を完了すると、後ほど、ダウンロードしたイメージを使用してアップグレードプロセスを開始できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 ファームウェア ダウンロードをセットアップします。



- 左側のナビゲーション ペインで[操作 (Operations)] > [サイト ファームウェア (Sites Firmware)] を選択します。
- メインウィンドウで [ダウンロード (Downloads)] タブを選択します。
- [ダウンロードのセットアップ (Setup Downloads)] タブをクリックします。

以前に 1 つ以上ダウンロードをセットアップしていた場合は、代わりに、メインペインの右上にある [ダウンロードのセットアップ (Setup Downloads)] ボタンをクリックします。

[イメージを APIC へダウンロード (Download Image to APIC)] 画面が表示されます。

ステップ 3 サイトを選択します。

ここで選択したすべてのサイトの Cisco APIC にイメージがダウンロードされます。

- [サイトの選択 (Select Sites)] をクリックします。
- [サイトの選択 (Select Sites)] ウィンドウで、1 つ以上のサイトをオンにし、[追加して閉じる (Add and Close)] をクリックします。
- [次へ (Next)] をクリックして続行します。

ステップ 4 詳細を入力します。

- a) **[名前 (Name)]** を入力します。
ダウンロードを追跡するためのわかりやすい名前を指定します。
- b) プロトコルを選択します。
HTTP または SCP 経由でイメージをダウンロードすることを選択できます。
- c) **[+ URLの追加 (+ Add URL)]** をクリックして、イメージの場所を指定します。
APIC とスイッチ ファームウェア イメージの両方を提供できます。
- d) **SCP** を選択した場合は、認証情報を入力します。
ログインする **[ユーザ名 (Username)]** (admin など) を入力する必要があります。
[認証タイプ (Authentication Type)] を選択します。
 - **パスワード認証**の場合は、前に指定したユーザ名のパスワードを入力します。
 - **SSH キー認証**の場合は、**SSH キー**と **SSH キー パスフレーズ**を入力する必要があります。
- e) **[次へ (Next)]** をクリックして続行します。

ステップ 5 確認画面で情報を確認し、**[送信 (Submit)]** をクリックして続行します。

表示される **[ダウンロード中 (Downloading)]** 画面で、イメージのダウンロードのステータスを確認できます。

ステータスをクリックして、進行状況の詳細を表示することもできます。

The screenshot displays the 'Image Download - MSO-d11' interface. At the top, there are three tabs: 'Setup', 'Downloading', and 'Complete'. The 'Downloading' tab is active. Below the tabs, the 'Download Details' section shows the overall status as 'Downloading' and a status breakdown with a count of 3. A table lists three sites: ifav109-site1, ifav109-site2, and ifav109-site3, each with 1 URL and a 'Downloading (1)' status. A right-hand pane for 'ifav109-site3' shows a 'Link' and a 'Status' bar at 30%.

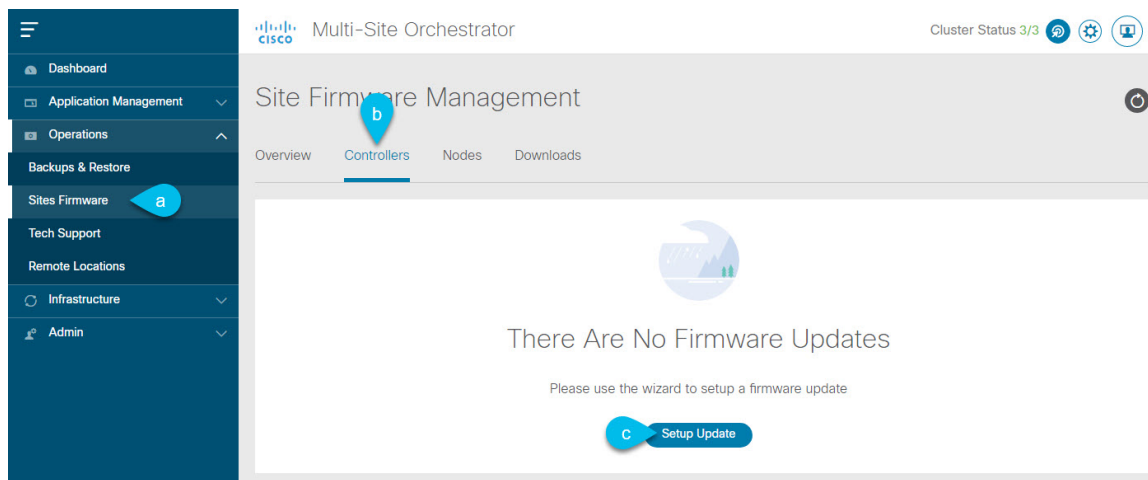
すべてのダウンロードが完了すると、[完了 (Completed)] 画面に移行します。[ダウンロード (Downloading)] 画面で待機する必要はありません。前の手順で指定したダウンロード名をクリックすると、[ダウンロード (Downloads)] タブからいつでも戻ることができます。

コントローラのアップグレード

ここでは、サイトの APIC クラスタのソフトウェアアップグレードを設定する方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 APIC クラスタのアップグレードをセットアップします。



- a) 左側のナビゲーションペインで[操作 (Operations)] > [サイト ファームウェア (Sites Firmware)] を選択します。
- b) メインウィンドウで [コントローラ (Controllers)] タブを選択します。
- c) [更新のセットアップ (Setup Update)] をクリックします。

以前に1つ以上の更新を設定している場合は、代わりにメインペインの右上にある [更新のセットアップ (Setup Update)] ボタンをクリックします。

[サイト ファームウェアの更新のセットアップ (Setup Site Firmware Update)] 画面が開きます。

ステップ3 アップグレードの詳細を入力します。

- a) [名前 (Name)] を入力します。

これは、いつでもアップグレードの進行状況を追跡するために使用できる、コントローラのアップグレードポリシー名です。
- b) [サイトの選択 (Select Sites)] をクリックします。

[サイトの選択 (Select Sites)] ウィンドウが表示されます。
- c) [サイトの選択 (Select Sites)] ウィンドウで、1つ以上のサイトをオンにし、[追加して閉じる (Add and Close)] をクリックします。
- d) [次へ (Next)] をクリックして続行します。

ステップ4 [バージョンの選択 (Version Selection)] 画面で、アップロードしたファームウェアバージョンを選択し、[次へ (Next)] をクリックします。

ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、[ファームウェアの更新のセットアップ (Setup Site Firmware Update)] 画面を閉じ、[操作 (Operations)] > [サイトのファームウェア (Sites Firmware)] > [コントローラ (Controllers)] タブに戻り、[更新 (Refresh)] ボタンをクリックして、使用可能な最新情報をリロードします。それからサイトのアップグレード手順をもう一度開始します。

ステップ5 [確認 (Validation)] 画面で情報を確認し、[次へ (Next)] をクリックします。

障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。

The screenshot shows the 'Setup Site Firmware Update' window with a progress bar at the top. The 'Validation' step is currently active, indicated by a blue circle with the number 3. Below the progress bar, a list of error messages is displayed for various sites:

- ifav109-site1**: Following nodes are not in vPC ['1111','102','101','104','103']. Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
- ifav109-site1**: Pod(s) [2] have fewer than two route reflectors for infra MP-BGP. Configure spine nodes as route reflector for infra MP-BGP. Make sure that at least one route reflector spine is always up by upgrading/downgrading them in separate groups.
- ifav109-site3**: Following nodes are not in vPC ['301','302']. Configure vPC for the listed leaf nodes to avoid traffic loss during the reboot of leaf nodes.
- ifav109-site3**: Pod(s) [1] have fewer than two route reflectors for infra MP-BGP. Configure spine nodes as route reflector for infra MP-BGP. Make sure that at least one route reflector spine is always up by upgrading/downgrading them in separate groups.
- ifav109-site3**: NTP is not configured. Configure NTP via System > QuickStart > First time setup of the ACI fabric > NTP. This is recommended to avoid any issues in database synchronization between nodes, SSL certificate check, etc.
- ifav109-site3**: APICs are not running recommended CIMC versions :node-1: 4.0(2f). Upgrade to the recommended CIMC version. APICs have recommended CIMC versions based on its hardware model and APIC firmware version.

At the bottom right of the window, there are 'Previous' and 'Next' buttons.

ステップ 6 [確認 (Confirmation)] 画面で情報を確認し、[送信 (Submit)] をクリックしてアップグレードを開始します。

ステップ 7 [インストールの準備完了 (Ready to Install)] 画面で、[インストール (Install)] をクリックします。

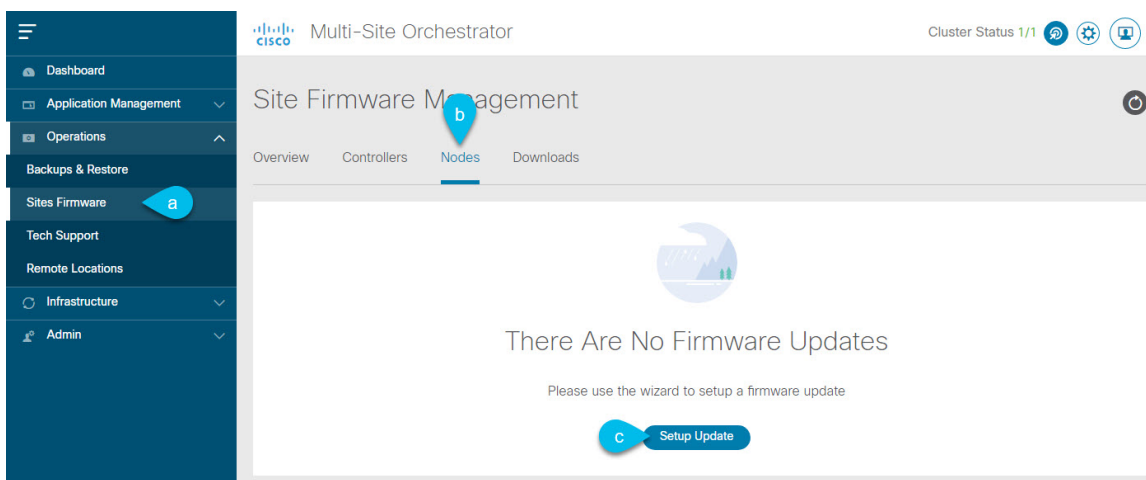
アップグレードプロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メインペインの右上にある [更新 (Refresh)] ボタンをクリックすると、手動で更新できます。

ノードのアップグレード

ここでは、サイトのスイッチ ノードのソフトウェア アップグレードを設定する方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 スイッチ ノードのアップグレードをセットアップします。



- a) 左側のナビゲーション ペインで[操作 (Operations)] > [サイト ファームウェア (Sites Firmware)]を選択します。
- b) メイン ウィンドウで [ノード (Node)] タブを選択します。
- c) [更新のセットアップ (Setup Update)] をクリックします。

以前に1つ以上の更新を設定している場合は、代わりにメインペインの右上にある[更新のセットアップ (Setup Update)] ボタンをクリックします。

[ノード ファームウェアの更新のセットアップ (Setup Node Firmware Update)] 画面が開きます。

ステップ 3 アップグレードの詳細を入力します。

- a) [名前 (Name)] を入力します。
これは、いつでもアップグレードの進行状況を追跡するために使用できるアップグレードポリシー名です。
- b) [ノードの選択 (Select Nodes)] をクリックします。
[ノードの選択 (Select Nodes)] ウィンドウが表示されます。
- c) サイトを選択し、そのサイトのスイッチノードを選択して、[追加して閉じる (Add and Close)] をクリックします。
一度に1つのサイトからスイッチノードを追加できます。他のサイトからスイッチを追加する場合は、この手順を繰り返します。
- d) 他のサイトのノードについて、前のサブステップを繰り返します。
- e) [次へ (Next)] をクリックして続行します。

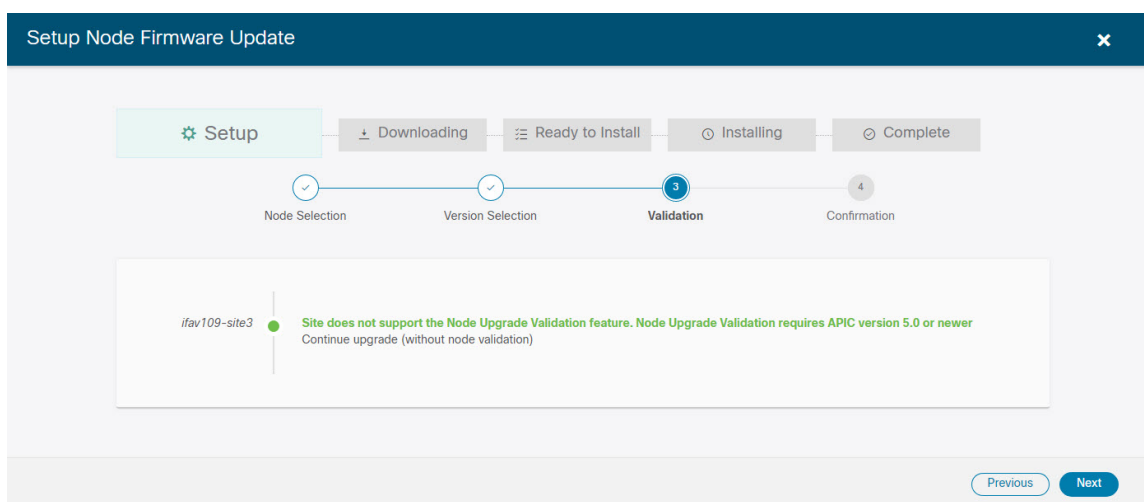
ステップ 4 [バージョンの選択 (Version Selection)] 画面で、アップロードしたファームウェア バージョンを選択し、[次へ (Next)] をクリックします。

ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、[ファームウェアの更新のセットアップ (Setup Site Firmware Update)] 画面を閉じ、[操作 (Operations)] > [サイトのファームウェア (Sites Firmware)] > [ノード (Nodes)] タブに戻り、[更新 (Refresh)] ボタンをクリックして、使用可能な最新情報をリロードします。それからサイトのアップグレード手順をもう一度開始します。

ステップ 5 [検証 (Validation)] 画面で、障害が発生していないことを確認し、[次へ (Next)] をクリックします。

障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。

(注) リリース 5.0(1) より前のリリースを実行しているサイトはノード検証をサポートしていないため、NDO からのアップグレードを開始する前に、サイトの APIC でスイッチ ノードの障害をチェックすることを推奨します。



ステップ 6 [確認 (Confirmation)] 画面で情報を確認し、[送信 (Submit)] をクリックして続行します。

これにより、選択したすべてのノードにイメージが事前にダウンロードされます。ダウンロードが完了すると、画面が [インストール準備完了 (Ready to Install)] に遷移し、次の手順に進むことができます。

ステップ 7 (オプション) [詳細設定 (Advanced Settings)] を変更します。

(注) 詳細オプションを変更する前に、[Upgrade and Downgrading the Cisco APIC and Switch Software \(Cisco APIC Installation, Upgrade, and Downgrade Guide\)](#) で説明されている Cisco APIC アップグレードプロセスのガイドライン、推奨事項、および制限事項を確認してください。

[インストールの準備完了 (Ready to Install)] 画面で、[詳細設定 (Advanced Settings)] メニューを開いて追加のオプションを表示できます。

- [互換性チェックを無視 (Ignore Compatibility Check)] : デフォルトでは、このオプションは [いいえ (No)] に設定され、互換性チェックが有効になっています。システムの現在実行中のバージョンから指定された新しいバージョンへのアップグレードパスがサポートされているかどうかを確認されます。

[互換性チェックを無視 (Ignore Compatibility Check)] フィールドで [はい (Yes)] にして互換性チェック機能を無効にした場合、システムでサポートされていないアップグレードが実行されるリスクがあり、システムが利用できない状態になる可能性があります。

- **[グレースフル チェック (Graceful Check)]** : デフォルトでは、このオプションは [いいえ (No)] に設定されています。アップグレードプロセスでのアップグレード実行前には、どのスイッチもグレースフル挿入/取り外し (GIR) モードになりません。

このオプションを有効にすると、アップグレードの実行中にノードをグレースフルに (GIRを使用して) ダウンさせることができ、アップグレードによるトラフィック損失が減少します。

- **[実行モード (Run Mode)]** : デフォルトでは、このオプションは [失敗時に続行 (Continue on Failure)] に設定されており、ノードのアップグレードが失敗すると、次のノードに進みます。または、このオプションを [失敗時に一時停止 (Pause on Failure)] に設定すると、いずれかのノードのアップグレードが失敗した場合にアップグレードプロセスを停止できます。

ステップ 8 [Failed] とマークされたノードをアップグレードから削除します。

アップグレードポリシーに、ファームウェアのダウンロードに失敗した1つ以上のノードが含まれている場合、アップグレードを続行できません。[失敗 (Failed)] ステータスにカーソルを合わせると、詳細情報と失敗の理由が表示されます。

アップグレードからノードを削除するには、[**アップデートの詳細を編集 (Edit Update Details)**] のリンク ([**インストールの準備完了 (Ready to Install)**] 画面) をクリックします。

ステップ 9 [**インストール (Install)**] をクリックしてアップグレードを開始します。

アップグレードプロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メインペインの右上にある [**更新 (Refresh)**] ボタンをクリックすると、手動で更新できます。



第 8 章

テクニカル サポート

- [テクニカル サポートおよびシステム ログ \(115 ページ\)](#)
- [システム ログのダウンロード \(116 ページ\)](#)
- [外部アナライザへのストリーミング システム ログ \(116 ページ\)](#)

テクニカル サポートおよびシステム ログ

Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

追加のツールを使用して重要なイベントを遅延なく迅速に解析、表示、応答する必要がある場合は、いつでも、ログをダウンロードするか、Splunk などの外部ログアナライザにストリーミングするかを選択できます。

リリース 3.3(1) 以降、テクニカル サポートログは 2 つの部分に分割されています。

- 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ ファイル
- 可読性を高めた、JSON ベースのデータベース バックアップ

各バックアップアーカイブには、次の内容が含まれています。

- `xxxx` : バックアップ時に使用可能なコンテナ ログ用の `xxxx` 形式の 1 つ以上のファイル。
- `msc-backup-<date>_temp` : 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ。
- `msc-db-json-<date>_temp` : JSON 形式のバックアップコンテンツ。

例 :

```
msc_anpEpgRels.json
msc_anpExtEpgRels.json
msc_asyncExecutionStatus.json
msc_audit.json
msc_backup-versions.json
msc_backupRecords.json
msc_ca-cert.json
msc_cloudSecStatus.json
```

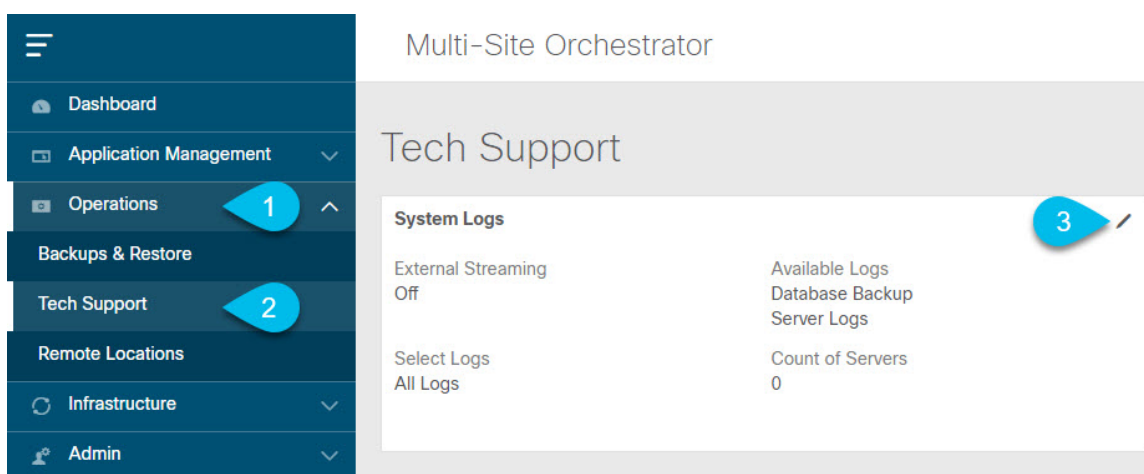
```
msc_consistency.json
...
```

システム ログのダウンロード

このセクションでは、Nexus Dashboard Orchestrator により管理されているすべてのスキーマ、サイト、テナント、およびユーザのトラブルシューティングレポートとインフラストラクチャログファイルを生成します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [システムログ (System Logs)] 画面を開きます。



- メインメニューで、[操作 (Operations)] > [テクニカル サポート (Tech Support)] を選択します。
- [システム ログ (System Logs)] フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 [ログのダウンロード (Download Log)] ボタンをクリックしてログをダウンロードします。

アーカイブがシステムにダウンロードされます。この章の最初のセクションで説明されているすべての情報を含んでいます。

外部アナライザへのストリーミング システム ログ

Nexus Dashboard Orchestrator を使用すると、Orchestrator ログを外部のログアナライザーツールにリアルタイムで送信できます。生成されたイベントをストリーミングすることにより、追加のツールを使用して、遅延なしで重要なイベントをすばやく解析、表示、および対応できます。

ここでは、Nexus Dashboard Orchestrator が外部アナライザーツール (Splunk や syslog など) にログをストリーミングできるようにする方法について説明します。

始める前に

- このリリースでは、外部ログアナライザーとして Splunk と syslog のみがサポートされています。
- このリリースでは、Application Services Engine 展開で Nexus Dashboard Orchestrator の syslog のみがサポートされます。
- このリリースは、最大 5 台の外部サーバをサポートします。
- Splunk を使用する場合は、ログアナライザー サービス プロバイダをセットアップして構成します。

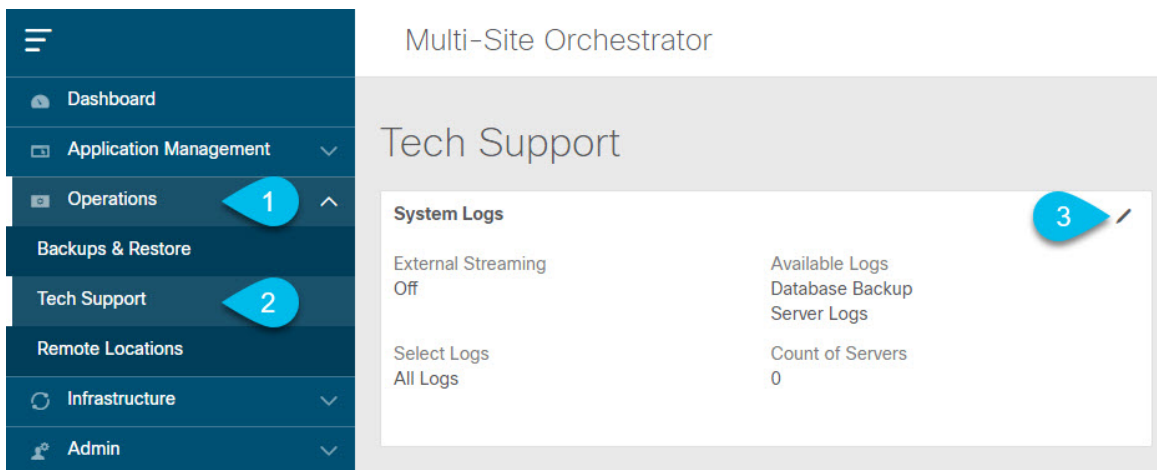
外部ログアナライザーの設定方法の詳細については、マニュアルを参照してください。

- Splunk を使用する場合は、サービス プロバイダの認証トークンを取得します。

Splunk サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、要するに、[設定 (Settings)] > [データ入力 (Data Inputs)] > [HTTP イベントコレクタ (Data input HTTP Event Collector)]を選択し、[新規トークン (New token)]をクリックして、認証トークンを取得できます。

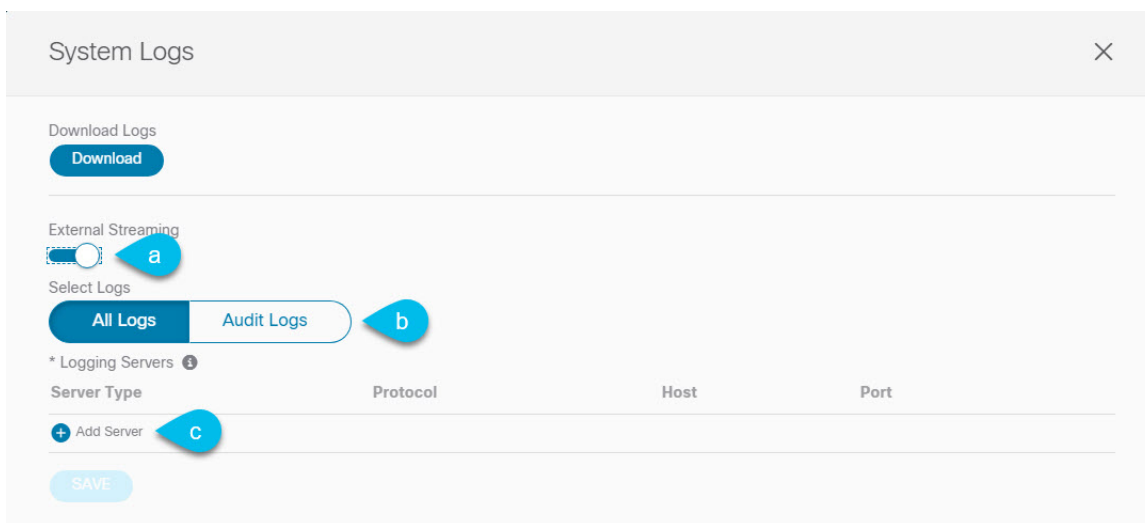
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [システムログ (System Logs)] 画面を開きます。



- メインメニューで、[操作 (Operations)] > [テクニカル サポート (Tech Support)]を選択します。
- [システム ログ (System Logs)] フレームの右上隅にある編集ボタンをクリックします。

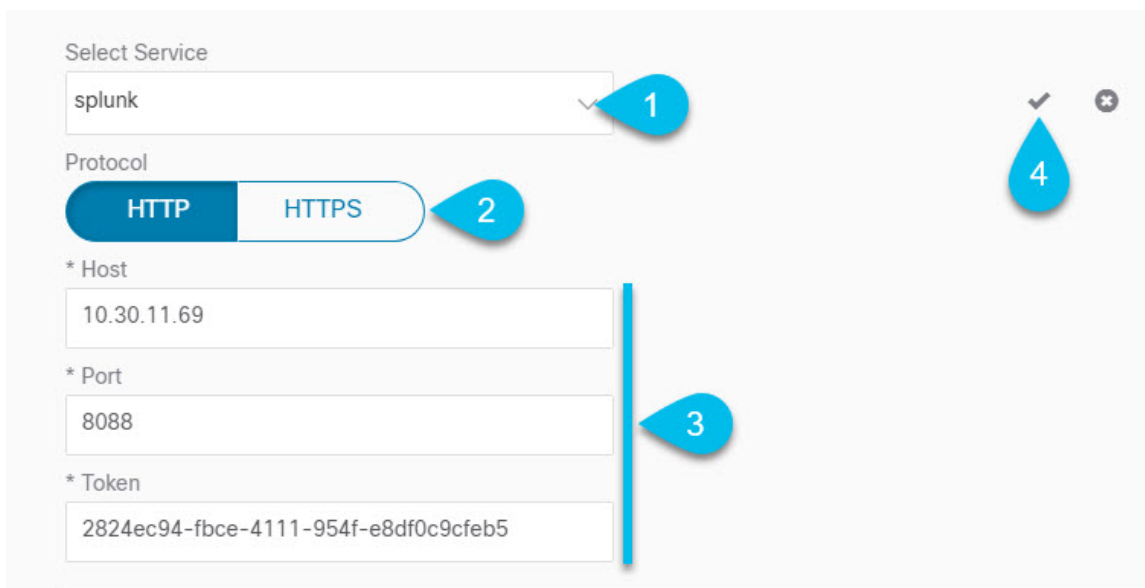
ステップ 3 [システムログ (System Logs)] ウィンドウで、外部ストリーミングを有効にし、サーバを追加します。



- 【外部ストリーミング (External Streaming)】ノブを有効にします。
- 【すべてのログ (All Logs)】をストリーミングするか、【監査ログ (Audit Logs)】のみをストリーミングするかを選択します。
- 【サーバーの追加 (Add Server)】をクリックして、外部ログアナライザサーバーを追加します。

ステップ 4 Splunk サーバーを追加します。

Splunk サービスを使用する予定がない場合は、この手順をスキップします。



- サーバーのタイプとして [Splunk] を選択します。
- プロトコルを選択します。
- Splunk サービスから取得したサーバ名または IP アドレス、ポート、および認証トークンを入力します。

Splunk サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、要するに、[設定 (Settings)] > [データ入力 (Data Inputs)] > [HTTP イベントコレクタ (HTTP Event Collector)] を選択し、[新規トークン (New token)] をクリックして、認証トークンを取得できます。

d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 5 syslog サーバーを追加します。

syslog を使用しない場合は、この手順をスキップします。

The screenshot shows a configuration form for adding a syslog server. The form has the following fields and callouts:

- Select Service:** A dropdown menu with 'syslog' selected. A blue callout bubble with the number '1' points to this field.
- Protocol:** Two radio buttons, 'TCP' and 'UDP'. 'UDP' is selected. A blue callout bubble with the number '2' points to this section.
- * Host:** A text input field containing '10.195.223.220'. A blue callout bubble with the number '3' points to this field.
- * Port:** A text input field containing '514'. A blue callout bubble with the number '3' points to this field.
- Severity:** A dropdown menu with 'Warning' selected. A blue callout bubble with the number '4' points to a checkmark icon in the top right corner of the form.

a) サーバーのタイプとして [syslog] を選択します。

b) プロトコルを選択します。

c) サーバー名または IP アドレス、ポート番号、およびストリーミングするログメッセージの重大度を指定します。

d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 6 複数のサーバーを追加する場合は、この手順を繰り返します。

このリリースは、最大 5 台の外部サーバ0をサポートします。

ステップ 7 [保存 (Save)] をクリックして、変更内容を保存します。

System Logs ×

Download Logs
[Download](#)

External Streaming

Select Logs
[All Logs](#) [Audit Logs](#)

* Logging Servers ⓘ

Server Type	Protocol	Host	Port	
splunk	http	10.30.11.69	8088	✖
syslog	tcp	10.195.223.220	514	✖

[+](#) Add Server

[SAVE](#)



第 III 部

インフラストラクチャ管理

- システム設定 (123 ページ)
- Nexus Dashboard での NDO サービスのアップグレード (125 ページ)
- Cisco ACI サイトの設定 (137 ページ)
- サイトの追加と削除 (145 ページ)
- インフラ一般設定 (153 ページ)
- Cisco APIC サイトのインフラの設定 (161 ページ)
- Cisco Cloud APIC サイトのインフラの設定 (169 ページ)
- ACI サイト向けのインフラ設定の展開 (173 ページ)
- CloudSec 暗号化 (179 ページ)



第 9 章

システム設定

- システム設定 (123 ページ)
- システム エイリアスとバナー (123 ページ)
- ログイン試行回数とロックアウト時間 (124 ページ)

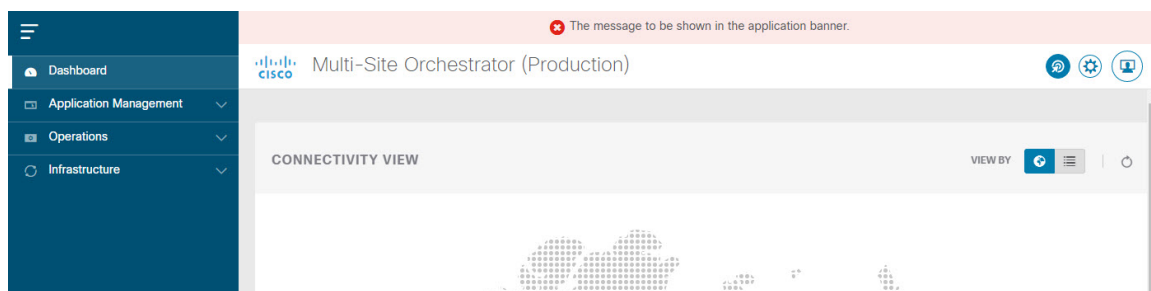
システム設定

次のセクションで説明するように、Multi-Site Orchestrator に対して設定できる、**管理 > システム設定**で使用可能なグローバルシステム設定が多数あります。

システム エイリアスとバナー

このセクションでは、Nexus Dashboard Orchestrator のエイリアスを設定する方法と、次の図に示すように、GUI全体で画面の上部に表示されるカスタムのバナーを有効にする方法について説明します。

図 13: システム バナーの表示



ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)] > [システム設定 (System Configuration)]** を選択します。

ステップ 3 **[編集 (Edit)]** のアイコンをクリックします。これは**[システム エイリアスとバナー System Alias & Banners]** 領域の右にあります。

[システム エイリアスとバナー System & Banners] の設定ウィンドウが表示されます。

ステップ4 [エイリアス (Alias)] フィールドで、システムのエイリアスを指定します。

ステップ5 GUI バナーを有効にするかどうかを選択します。

ステップ6 バナーを有効にする場合には、バナーに表示されるメッセージを指定する必要があります。

ステップ7 バナーを有効にする場合には、バナーの重大度を意味する色を選択する必要があります。

ステップ8 [保存 (Save)] をクリックして、変更内容を保存します。

ログイン試行回数とロックアウト時間

Orchestrator がログイン試行を連続して失敗したことが検出されると、そのユーザは、不正アクセスを防ぐために、システムからロックアウトされます。ログイン試行が失敗した場合の処理方法は設定できます。たとえば、何回失敗するとロックアウトされるか、およびロックアウトの長さなどがあります。



(注) この機能は、リリース 2.2(1) 以降を最初にインストールしたとき、アップグレードしたときにデフォルトで有効になります。

ステップ1 Orchestrator にログインします。

ステップ2 左側のナビゲーションペインから[管理 (Admin)] > [システム設定 (System Configuration)] を選択します。

ステップ3 [試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)] エリアの右側にある [編集 (Edit)] アイコンをクリックします。

これにより、[試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)] 設定ウィンドウが表示されます。

ステップ4 [試行の失敗の設定 (Fail Attempts Settings)] ドロップダウンから、ユーザが何回試行に失敗するとロックアウトされるかを選択します。

ステップ5 [ロックアウト時間(分)(Lockout Time (Minutes))] ドロップダウンから、ロックアウトの長さを選択します。

これは、トリガーされた後の、基本的なロックアウト期間を指定します。このタイマーは、さらにログイン試行が連続して失敗するたびに、3 ずつ延長されます。

ステップ6 [保存 (Save)] をクリックして、変更内容を保存します。



第 10 章

Nexus Dashboard での NDO サービスのアップグレード

- [概要 \(125 ページ\)](#)
- [前提条件とガイドライン \(125 ページ\)](#)
- [Cisco App Store を使用した NDO サービスのアップグレード \(127 ページ\)](#)
- [NDO サービスの手動アップグレード \(129 ページ\)](#)
- [設定のばらつきの解決とテンプレートの再展開 \(131 ページ\)](#)

概要

以下のセクションでは、Cisco Nexus ダッシュボードに展開されている Cisco Nexus Dashboard Orchestrator をアップグレードまたはダウングレードする方法について説明します。

VMware ESX VM または Cisco Application Services Engine に導入されている以前のリリースを実行している場合は、代わりに、[Cisco Nexus Dashboard Orchestrator 展開ガイド](#)の「Nexus ダッシュボードへの既存のクラスタの移行」の章の説明に従って、まったく新しいクラスタを展開し、既存のクラスタから設定を転送する必要があります。

前提条件とガイドライン

Cisco Nexus Dashboard Orchestrator クラスタをアップグレードまたはダウングレードする前に、次の手順を実行します。

- リリース 3.2(1) より前のリリースからのステートフルアップグレードはサポートされていません。

それより前のリリースからアップグレードする場合は、この章の残りの部分をスキップし、[『12.0.1a12.0.2fNexus Dashboard Orchestrator Deployment Guide』](#)の「Migrating Existing Cluster to Nexus Dashboard」の章に記載されている手順に従ってください。

- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

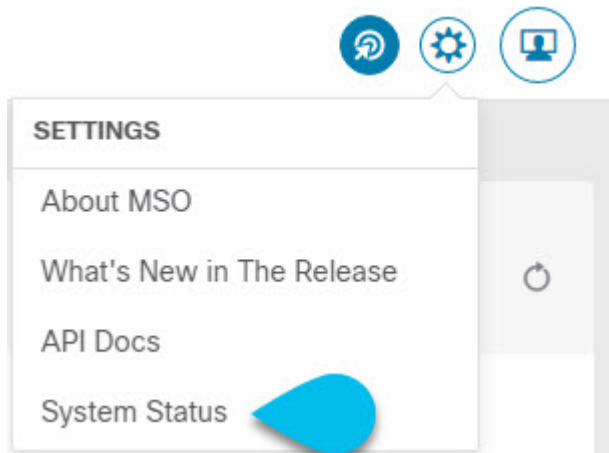
Nexus ダッシュボードクラスタの状態は、次の 2 つの方法のいずれかで確認できます。

- Nexus ダッシュボード GUI にログインし、[システム概要 (System Overview)] ページでシステムステータスを確認します。
- いずれかのノードに直接 `rescue-user` としてログインし、次のコマンドを実行します。

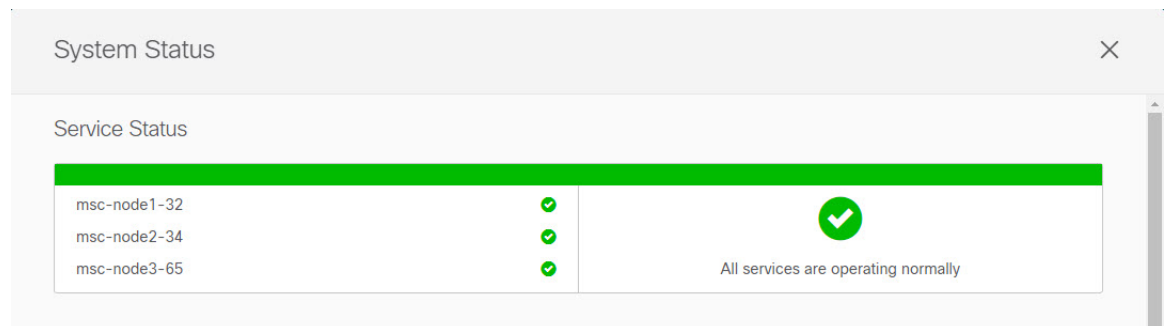
```
# acs health
All components are healthy
```

- 現在の Cisco Nexus Dashboard Orchestrator が正常に動作していることを確認します。

Nexus Dashboard Orchestrator サービスのステータスは、[設定 (Settings)] > [システムステータス (System Status)] に移動して確認できます。



次に、すべてのノードとサービスのステータスが正常であることを確認します。



- NDO サービスのアップグレードは次のいずれかの方法で実行できます。
 - [Cisco App Store を使用した NDO サービスのアップグレード \(127 ページ\)](#) の説明に従って、Nexus ダッシュボードの App Store を使用します。
この場合、Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus ダッシュボードから到達可能である必要があります。Nexus ダッシュボードのプロキシ設定については、『*Nexus Dashboard User Guide*』を参照してください。



(注) App Storeでは、サービスの最新バージョンにのみアップグレードできます。たとえば、リリース 3.7(1) が利用可能な場合は、App Storeを使用してそれより前のリリースにアップグレードすることはできません。別のリリースにアップグレードするには、以下で説明する手動アップグレードプロセスを使用する必要があります。

- [NDO サービスの手動アップグレード \(129 ページ\)](#) の説明に従って、新しいアプリケーションイメージを手動でアップロードします。

この方法は、DC App Center への接続を確立できない場合、または使用可能な最新リリースではないアプリケーションのバージョンにアップグレードする場合に使用できます。

- Nexus Dashboard Orchestrator をこのリリースにアップグレードした後に新しい Cloud APIC サイトを追加および管理する場合は、それらのサイトが Cloud APIC リリース 5.2(1) 以降を実行していることを確認してください。

以前のリリースを実行しているクラウド APIC サイトのオンボーディングと管理はサポートされていません。

- リリース 3.3(1) より前のリリースへのダウングレードはサポートされていません。
- アップグレードを開始する前に、既存の構成をバックアップすることをお勧めします。

Cisco App Store を使用した NDO サービスのアップグレード

ここでは、Cisco Nexus Dashboard Orchestrator をアップグレードする方法について説明します。

始める前に

- [前提条件とガイドライン \(125 ページ\)](#) で説明している前提条件をすべて満たしていることを確認します。
- Cisco DC App Center が Nexus ダッシュボードから管理ネットワーク経由で直接、またはプロキシ設定を使用して到達可能であることを確認します。

Nexus ダッシュボードのプロキシ設定については、[『Nexus Dashboard User Guide』](#) を参照してください。

ステップ 1 Nexus Dashboard にログインします。

ステップ 2 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。

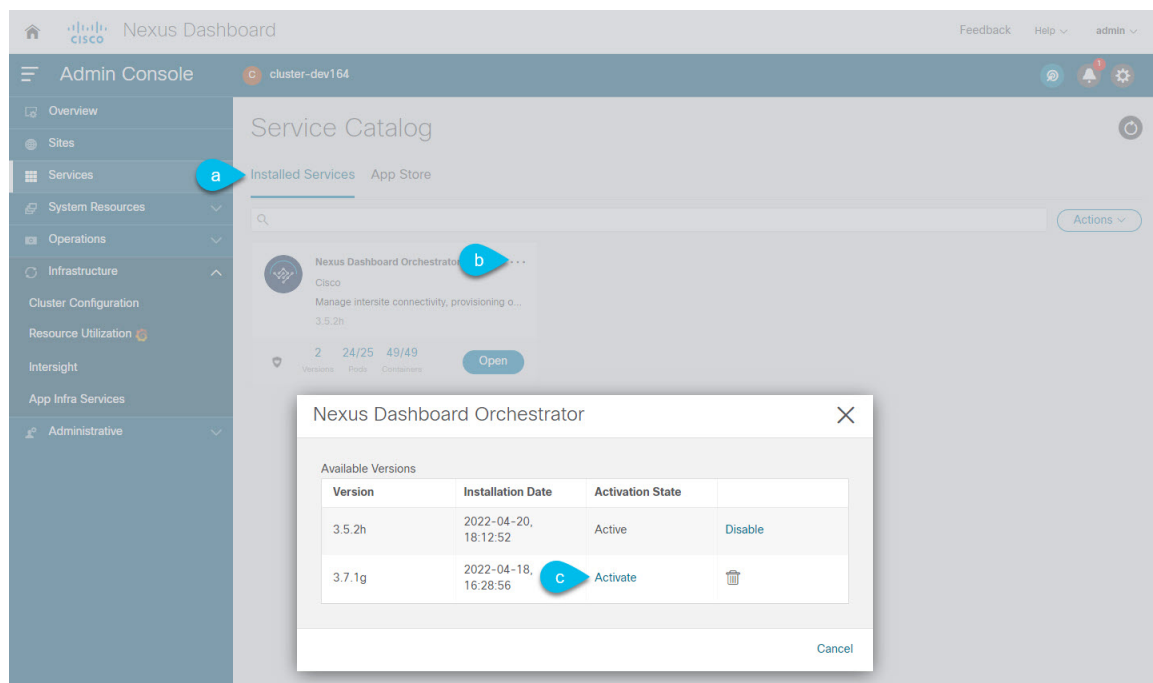
ステップ 3 App Store を使用してアプリケーションをアップグレードします。

- [サービス カタログ (Service Catalog)]** 画面で **[アプリストア (App Store)]** タブを選択します。
- [Nexus ダッシュボード オーケストレータ (Nexus Dashboard Orchestrator)]** タイルで、**[アップグレード (Upgrade)]** をクリックします。
- 開いた **[ライセンス契約 (License Agreement)]** ウィンドウで、**[同意してダウンロード (Agree and Download)]** をクリックします。

ステップ 4 新しいイメージが初期化されるまで待ちます。

新しいアプリケーションイメージが使用可能になるまでに最大 20 分かかることがあります。

ステップ 5 新しい画像をアクティブにします。



- [サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。
- [Nexus Dashboard Orchestrator]** タイルの右上にあるメニュー (...) をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。
- [Available Versions]** ウィンドウで、新しいイメージの横にある **[アクティベート (Activate)]** をクリックします。

(注) 新しいイメージをアクティブにする前に、現在実行中のイメージを無効にしないでください。イメージアクティベーションプロセスは、現在実行中のイメージを認識し、現在実行中のバージョンに必要なアップグレードワークフローを実行します。

すべてのアプリケーションサービスが起動し、GUIが使用可能になるまでに、さらに最大20分かかる場合があります。このページは、プロセスが完了した時点で自動的に再ロードされます。

ステップ6 (任意) 古いアプリケーション イメージを削除します。

ダウングレードする場合に備えて、古いアプリケーションバージョンを保持しておくこともできます。または、この手順の説明に従って削除することもできます。

- a) [サービス カタログ (Service Catalog)] 画面で、[インストール済みサービス (Installed Services)] タブを選択します。
- b) [Nexus Dashboard Orchestrator] タイルの右上にあるメニュー (...) をクリックし、[利用可能なバージョン (Available Versions)] を選択します。
- c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

ステップ7 アプリを起動します。

アプリケーションを起動するには、Nexus ダッシュボードの [サービスカタログ (Service Catalog)] ページのアプリケーションタイルで [開く (Open)] をクリックします。

シングルサインオン (SSO) 機能を使用すると、Nexus ダッシュボードで使用したものと同一クレデンシャルを使用してアプリケーションにログインできます。

次のタスク

NDO サービスをアップグレードした後、構成のばらつきを解決し、「[設定のばらつきの解決とテンプレートの再展開 \(131 ページ\)](#)」で説明されているようにテンプレートを再展開する必要があります。

NDO サービスの手動アップグレード

ここでは、Cisco Nexus Dashboard Orchestrator をアップグレードする方法について説明します。

始める前に

- [前提条件とガイドライン \(125 ページ\)](#) で説明している前提条件をすべて満たしていることを確認します。

ステップ1 ターゲットのリリース イメージをダウンロードします。

- a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
<https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html>
- b) [バージョン (Version)] ドロップダウンから、インストールするバージョンを選択し、[ダウンロード (Download)] をクリックします。
- c) [同意してダウンロード (Agree and download)] をクリックしてライセンス契約に同意し、イメージをダウンロードします。

ステップ2 Nexus Dashboard にログインします。

ステップ3 Nexus ダッシュボードにイメージをアップロードします。

- a) 左のナビゲーションメニューから [サービス カタログ (Service Catalog)] を選択します。
- b) Nexus ダッシュボードの [サービス カタログ (Service Catalog)] 画面で、[インストール済みサービス (Installed Services)] タブを選択します。
- c) メインペインの右上にある [アクション (Actions)] メニューから、[アプリケーションのアップロード (Upload App)] を選択します。
- d) [アプリケーションのアップロード (Upload App)] ウィンドウで、イメージの場所を選択します。
アプリケーションイメージをシステムにダウンロードした場合は、[ローカル (Local)] を選択します。
サーバでイメージをホストしている場合は、[リモート (Remote)] を選択します。
- e) ファイルを選択します。
前のサブステップで [ローカル (Local)] を選択した場合は、[ファイルの選択 (Select File)] をクリックし、ダウンロードしたアプリケーションイメージを選択します。
[リモート (Remote)] を選択した場合は、イメージファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。
- f) [アップロード (Upload)] をクリックして、アプリケーションをクラスタに追加します。
アップロードの進行状況バーとともに新しいタイルが表示されます。イメージのアップロードが完了すると、Nexus ダッシュボードは新しいイメージを既存のアプリケーションとして認識し、新しいバージョンとして追加します。

ステップ 4 新しいイメージが初期化されるまで待ちます。

新しいアプリケーションイメージが使用可能になるまでに最大 20 分かかることがあります。

ステップ 5 新しい画像をアクティブにします。

The screenshot shows the Nexus Dashboard interface. The left sidebar contains the navigation menu with 'Services' highlighted. The main area displays the 'Service Catalog' with the 'Installed Services' tab selected. A modal window titled 'Nexus Dashboard Orchestrator' is open, showing a table of available versions. The table has columns for Version, Installation Date, and Activation State. The current version 3.7.1g is highlighted with a blue circle 'c' next to its 'Activate' button.

Version	Installation Date	Activation State
3.5.2h	2022-04-20, 18:12:52	Active Disable
3.7.1g	2022-04-18, 16:28:56	Activate Cancel

- a) [サービス カタログ (Service Catalog)] 画面で、[インストール済みサービス (Installed Services)] タブを選択します。
- b) [Nexus Dashboard Orchestrator] タイルの右上にあるメニュー (...) をクリックし、[利用可能なバージョン (Available Versions)] を選択します。
- c) [Available Versions] ウィンドウで、新しいイメージの横にある [アクティベート (Activate)] をクリックします。

(注) 新しいイメージをアクティブにする前に、現在実行中のイメージを無効にしないでください。イメージ アクティベーション プロセスは、現在実行中のイメージを認識し、現在実行中のバージョンに必要なアップグレードワークフローを実行します。

すべてのアプリケーションサービスが起動し、GUIが使用可能になるまでに、さらに最大20分かかる場合があります。このページは、プロセスが完了した時点で自動的に再ロードされます。

ステップ 6 (任意) 古いアプリケーションイメージを削除します。

ダウングレードする場合に備えて、古いアプリケーションバージョンを保持しておくこともできます。または、この手順の説明に従って削除することもできます。

- a) [サービス カタログ (Service Catalog)] 画面で、[インストール済みサービス (Installed Services)] タブを選択します。
- b) [Nexus Dashboard Orchestrator] タイルの右上にあるメニュー (...) をクリックし、[利用可能なバージョン (Available Versions)] を選択します。
- c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

ステップ 7 アプリを起動します。

アプリケーションを起動するには、Nexus ダッシュボードの [サービスカタログ (Service Catalog)] ページのアプリケーションタイルで [開く (Open)] をクリックします。

シングルサインオン (SSO) 機能を使用すると、Nexus ダッシュボードで使用したものと同一のクレデンシャルを使用してアプリケーションにログインできます。

次のタスク

NDO サービスをアップグレードした後、構成のばらつきを解決し、「[設定のばらつきの解決とテンプレートの再展開 \(131 ページ\)](#)」で説明されているようにテンプレートを再展開する必要があります。

設定のばらつきの解決とテンプレートの再展開

いくつかの事例では、構成がサイトコントローラで実際に展開される状況が、Nexus Dashboard Orchestrator で定義された設定と異なる場合があります。これらの構成の不一致は、[構成のばらつき (Configuration Drifts)] と呼ばれ、次の図に示すように、スキーマビューのテンプレート名の横に黄色の注意サインで示されます。

Nexus Dashboard Orchestrator のこのリリースにアップグレードした後、アップグレード時のデータベース変換により生じる構成のばらつきがないことを確認してから、すべてのテンプレートを再展開してアップグレードを完了する必要があります。



(注) 構成のばらつきを解決する前にテンプレートを展開すると、Orchestrator で定義された構成がプッシュされ、ファブリックのコントローラで定義された値が上書きされます。

始める前に

Cisco App Store を使用した NDO サービスのアップグレード (127 ページ) または NDO サービスの手動アップグレード (129 ページ) の説明に従って、Nexus Dashboard Orchestrator をアップグレードしておく必要があります。

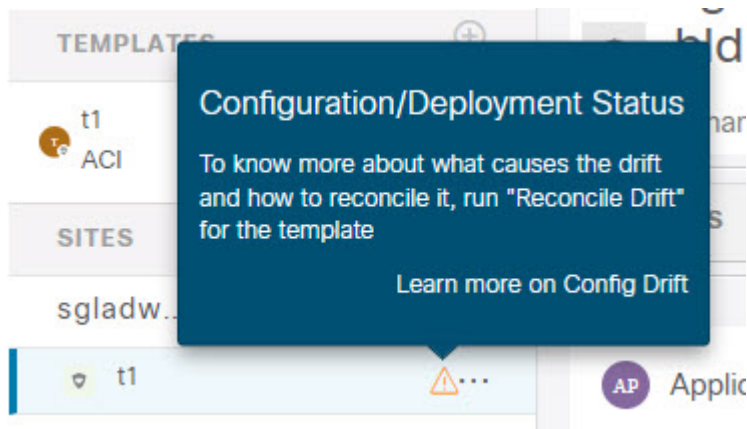
ステップ 1 Nexus Dashboard Orchestrator で、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] に移動します。

ステップ 2 最初のスキーマを選択し、そのテンプレートで構成ドリフトを確認します。

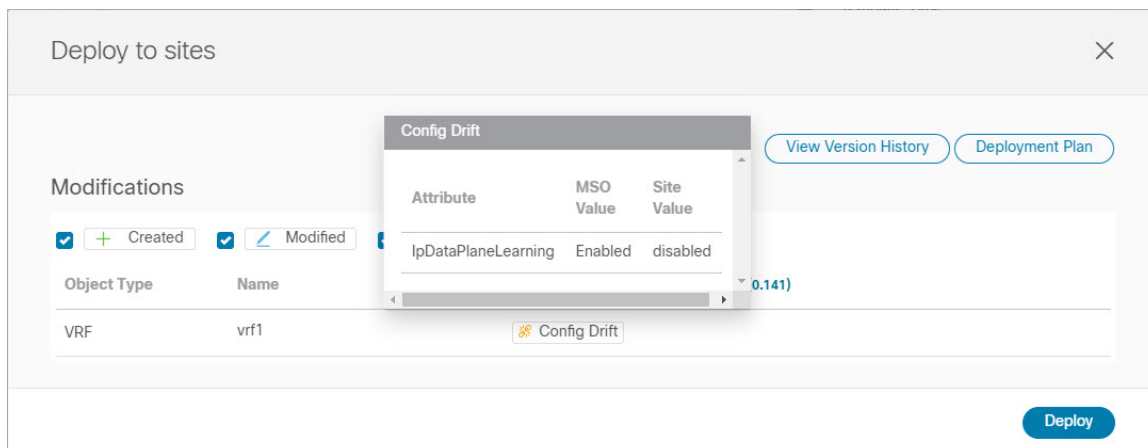
展開内のすべてのスキーマとテンプレートについて、次の手順を繰り返します。

次の 2 つの方法のいずれかで、構成のばらつきを確認できます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータスアイコンを確認します。



- テンプレートを選択し、[サイトへの展開 (Deploy to sites)] をクリックして構成比較画面を呼び出し、構成のばらつきが含まれているオブジェクトを確認します。



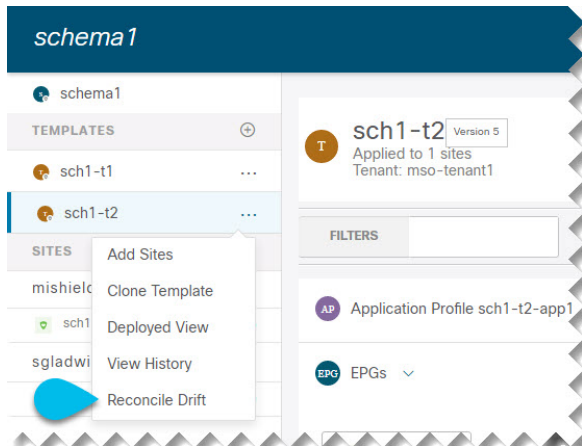
ステップ 3 テンプレートに構成のばらつきが含まれている場合は、競合を解決します。

構成のばらつきの詳細については、『[Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics](#)』の「構成のばらつき」の詳細を確認してください。

a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

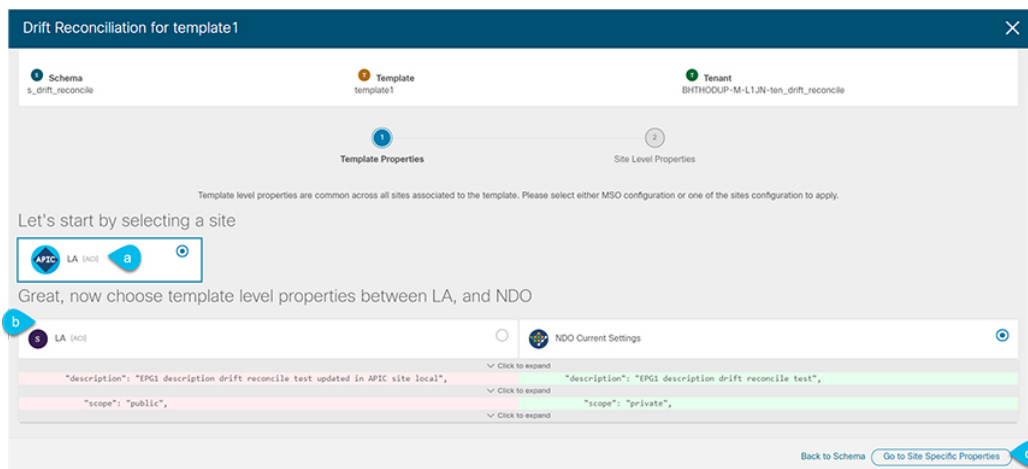
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

b) テンプレートの **[アクション (Actions)]** メニューから、**[ばらつきの調整 (Reconcile Drift)]** を選択します。



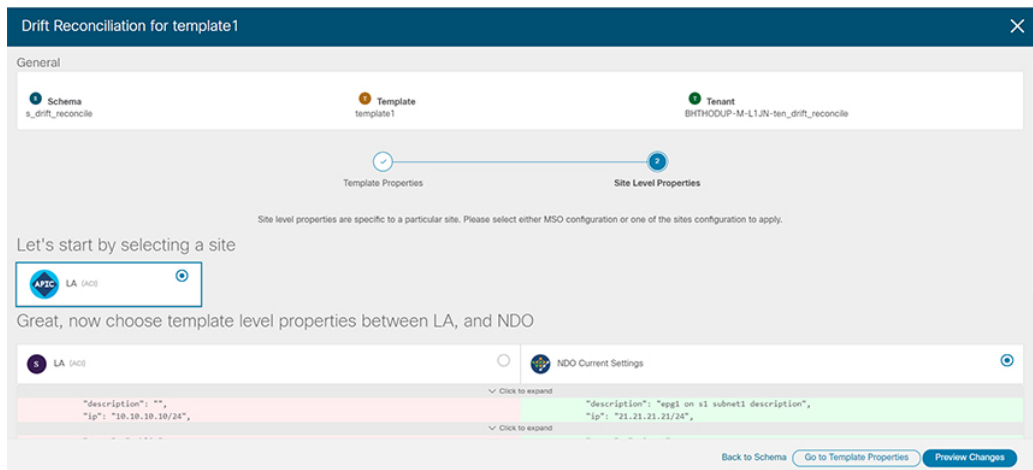
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

c) **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレートレベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変更されますが、Nexus Dashboard Orchestrator 構成を選択した場合は、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま保持されます。

- d) [サイト固有のプロパティに移動 (Go to Site Specific Properties)] をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカルプロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルの構成とサイトレベルの構成のどちらでも同じ選択を行います。ばらつきへの調整ウィザードでは、サイトのコントローラで定義されている構成を「テンプレートのプロパティ」レベルで選択し、Nexus Dashboard Orchestrator で定義された構成を「サイトのローカルプロパティ」レベルで選択したり、またその逆で選択したりすることもできます。

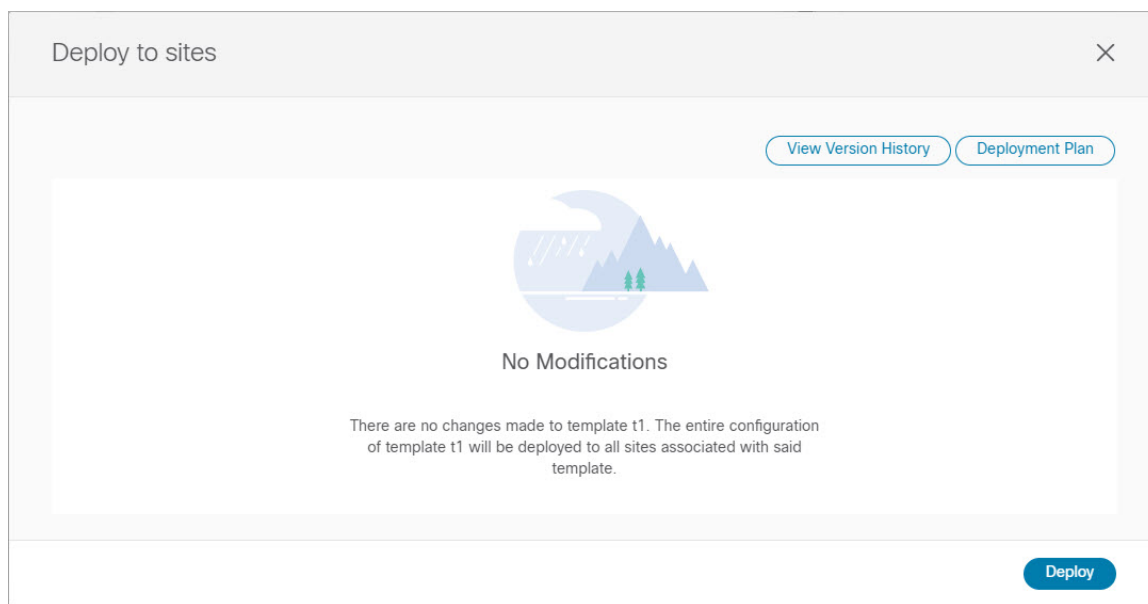
- e) [変更のプレビュー (Preview Changes)] をクリックして、選択内容を確認します。

プレビューは[ばらつきの調整 (Reconcile Drift)] ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、[サイトに展開 (Deploy to site)] をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

ステップ 4 すべての構成のばらつきが解決され、[サイトへの展開 (Deploy to sites)] ダイアログに変更が表示されなくなったら、テンプレートの完全な再展開を実行します。

(注) リリース 3.7(1) のデータベース変換のため、各テンプレートの完全な再展開を実行する必要があります。

次の図に示すように、[サイトへの展開 (Deploy to sites)] ダイアログに変更が含まれていないことを確認し、[展開 (Deploy)] をクリックして、完全な構成を再展開します。



ステップ 5 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 6 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション (Operations)] タブの監査ログを表示できます。

[監査ログ (Audit Logs)] ページで、すべてのテンプレートが [再展開済み (Redeployed)] と表示され、完全な再展開が正常に完了したことを確認します。



第 11 章

Cisco ACI サイトの設定

- [ポッドプロファイルとポリシーグループ \(137 ページ\)](#)
- [すべての APIC サイトのファブリック アクセス ポリシーの設定 \(138 ページ\)](#)
- [リモートリーフスイッチを含むサイトの設定 \(142 ページ\)](#)
- [Cisco Mini ACI ファブリック \(144 ページ\)](#)

ポッドプロファイルとポリシーグループ

各サイトの APIC には、ポッドポリシーグループを持つポッドプロファイルが 1 つ必要です。サイトにポッドポリシーグループがない場合は、作成する必要があります。通常、これらの設定はすでに存在していて、ファブリックを最初に展開したときに設定したとおりになっているはずです。

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッドプロファイルにポッドポリシーグループが含まれているかどうかを確認します。

[**ファブリック (Fabric)**] > [**ファブリック ポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**プロファイル (Profiles)**] > [**ポッドのプロファイルのデフォルト (Pod Profile default)**] に移動します。

ステップ 3 必要であれば、ポッドポリシーグループを作成します。

- [**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)**] に移動します。
- [**ポリシーグループ (Policy Groups)**] を右クリックし、[**ポッドポリシーグループの作成 (Create Pod Policy Groups)**] を選択します。
- 適切な情報を入力して、[**Submit**] をクリックします。

ステップ 4 新しい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割り当てます。

- [**ファブリック (Fabric)**] > [**ファブリック ポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**プロファイル (Profiles)**] > [**ポッドプロファイルのデフォルト (Pod Profile default)**] に移動します。
- デフォルトのプロファイルを選択します。
- 新しいポッドポリシーグループを選択し、[**更新 (Update)**] をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

APIC ファブリックを Nexus Dashboard Orchestrator に追加し、Nexus Dashboard Orchestrator により管理できるようにするには、サイトごとに設定することが必要な、ファブリック固有の多数のアクセス ポリシーがあります。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard Orchestrator に追加し、管理する前に、APIC サイトごとに作成する必要があるグローバルファブリックアクセスポリシーの設定について説明します。

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メインナビゲーションメニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。

サイトを Nexus Dashboard Orchestrator に追加するには、いくつかのファブリックポリシーを設定する必要があります。APIC の観点からは、ベアメタルホストを接続していた場合と同様に、ドメイン、AEP、ポリシーグループ、およびインターフェイスセレクトアを設定することができます。同じマルチサイトドメインに属するすべてのサイトに対して、スパインスイッチインターフェイスをサイト間ネットワークに接続するための同じオプションを設定する必要があります。

ステップ 3 VLAN プールを指定します。

最初に設定するのは、VLAN プールです。レイヤ3サブインターフェイスはVLAN4を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

- 左側のナビゲーションツリーで、[プール (Pools)] > [VLAN] を参照します。
- [VLAN] カテゴリを右クリックし、[VLAN プールの作成 (Create VLAN Pool)] を選択します。

[VLAN プールの作成 (CREATE VLAN Pool)] ウィンドウで、次の項目を指定します。

- [名前 (name)] フィールドで、VLAN プールの名前 (たとえば、msite) を指定します。
- [Allocation Mode (割り当てモード)] の場合は、[スタティック割り当て (Static Allocation)] を指定します。
- [Encap ブロック (Encap Blocks)] の場合は、単一の VLAN 4 だけを指定します。両方の [Range (範囲)] フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

ステップ 4 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

- 左側のナビゲーションツリーで、[グローバルポリシー (Global Policies)] > [接続可能なアクセス エンティティ プロファイル (Attachable Access Entity Profiles)] を参照します。

- b) [接続可能なアクセス エンティティ プロファイル (Attachable Access Entry Profiles)] 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 (Create Attachable Access Entity Profiles)] を選択します。

[接続可能アクセス エンティティ プロファイルの作成(Create Attachable Access Entity Profiles)] ウィンドウで、AEP の名前 (例: msite-aep) を指定します。

- c) [次へ(Next)] をクリックして [送信(Submit)] します。

インターフェイスなどの追加の変更は必要ありません。

ステップ5 ドメインを設定します。

設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestratorから選択するものになります。

- a) ナビゲーションツリーで、[物理的ドメインと外部ドメイン (Physical and External Domains)] > [外部でルーテッドドメイン (External Routed Domains)] を参照します。
- b) [外部ルーテッドドメイン(External Routed Domains)] カテゴリを右クリックし、[レイヤ3ドメインの作成 (Create Layer 3 Domain)] を選択します。

[レイヤ3ドメインの作成 (Create Layer 3 Domain)] ウィンドウで、次の項目を指定します。

- [名前 (name)] フィールドで、ドメインの名前を指定します。たとえば、msite-13です。
 - 関連付けられている接続可能エンティティ プロファイルの場合は、ステップ4で作成したAEPを選択します。
 - VLAN プールの場合は、ステップ3で作成したVLAN プールを選択します。
- c) [送信 (Submit)] をクリックします。

セキュリティドメインなどの追加の変更は必要ありません。

次のタスク

グローバルアクセスポリシーを設定した後も、[ファブリック アクセス インターフェイス ポリシーの設定 \(139ページ\)](#) の説明に従って、インターフェイスポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

始める前に

サイトの APIC では、[ファブリック アクセス グローバル ポリシーの設定 \(138 ページ\)](#) の説明に従って、VLAN プール、AEP、およびドメインなどのグローバルファブリック アクセス ポリシーを設定しておく必要があります。

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メインナビゲーションメニューから、**[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)]** を選択します。

前のセクションで設定した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

ステップ 3 スパイン ポリシー グループを設定します。

a) 左ナビゲーションツリーで、**[インターフェイス ポリシー (Interface Policie)] > [ポリシー グループ (Policy Groups)] > [スパイン ポリシー グループ (Spine Policy Groups)]** を参照します。

これは、ベアメタルサーバを追加する方法と類似していますが、リーフポリシーグループの代わりにスパイン ポリシー グループを作成する点が異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリを右クリックして、**[スパイン アクセス ポート ポリシー グループの作成 (Create Spine Access Port Policy Group)]** を選択します。

[スパイン アクセス ポリシー グループの作成 (Create Spine Access Port Policy Group)] ウィンドウで、以下のとおり指定します。

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば Spine1-PolGrp です。
- **[リンク レベル ポリシー (Link Level Policy)]** フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profil)]** の場合、前のセクションで設定した AEP を選択します。たとえば msite-aep です。

c) **[送信 (Submit)]** をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

a) 左ナビゲーションツリーで、**[インターフェイス ポリシー (Interface Policies)] > [ポリシー グループ (Profiles)] > [スパイン ポリシー グループ (Spine Profiles)]** を参照します。

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前 (Spine1など) を指定します。
- **[インターフェイス セレクタ (Interface Selectors)]**では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、**[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)]** ウィンドウで、次のように指定します。
 - **[名前 (name)]** フィールドに、ポートセレクタの名前を指定します (例: Spine1)。
 - **[インターフェイス ID (Interface IDs)]** に、ISN に接続するスイッチ ポートを指定します (例 5/32)。
 - **[インターフェイス ポリシー グループ (Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: Spine1-PolGrp)。

それから、**[OK]** をクリックして、ポートセレクタを保存します。

- c) **[送信 (Submit)]** をクリックしてスパイン インターフェイス プロファイルを保存します。

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

- a) 左ナビゲーションツリーで、**[スイッチ ポリシー (Switch Policies)]** > **[プロファイル (Profiles)]** > **[スパイン プロファイル (Spine Profiles)]** を参照します。
- b) **[スパイン プロファイル (Spine Profiles)]** カテゴリを右クリックし、**[スパイン プロファイルの作成 (Create Spine Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のように指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前を指定します (例: Spine1)。
 - **[スパインセレクタ (Spine Selector)]**で、**[+]** をクリックしてスパインを追加し、次の情報を入力します。
 - **[名前 (name)]** フィールドで、セレクタの名前を指定します (例: Spine1)。
 - **[ブロック (Blocks)]** フィールドで、スパイン ノードを指定します (例: 201)。
- c) **[更新 (Update)]** をクリックして、セレクタを保存します。
- d) **[次へ (Next)]** をクリックして、次の画面に進みます。
- e) 前の手順で作成したインターフェイス プロファイルを選択します。
たとえば、Spine1-ISNなどです。
- f) **[完了 (Finish)]** をクリックしてスパイン プロファイルを保存します。

リモート リーフ スイッチを含むサイトの設定

Multi-Site アーキテクチャはリモート リーフスイッチを持つ APIC サイトをサポートします。次のセクションでは、Nexus Dashboard Orchestrator がこれらのサイトを管理できるようにするために必要な注意事項、制限事項、および設定手順を説明します。

リモート リーフの注意事項と制限事項

Nexus Dashboard Orchestrator により管理されるリモート リーフをもつ APIC サイトを追加する場合、次の制約が適用されます。

- Cisco APICはリリース 4.2(4) 以降にアップグレードする必要があります。
- このリリースでは、物理リモート リーフ スイッチのみがサポートされます
- -EX および -FX 以降のスイッチのみが、マルチサイトで使用するリモートリーフスイッチとしてサポートされています。
- リモートリーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません
- 1つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません
- あるサイトと別のサイトのリモート リーフ間のブリッジ ドメインの拡張はサポートされていません。

また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

- 次の項で説明するように、リモートリーフの直接通信をイネーブルAPICにし、サイト内でルーティング可能なサブネットを直接設定する必要があります。
- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、Cisco APIC ノードのルーティング可能な IP アドレスを追加する必要があります。

各 APIC ノードのルーティング可能な IP アドレスは、[ルーティング可能 IP (Routable IP)] フィールド (APIC GUI の [システム (System)] > [コントローラ (Controllers)] > <コントローラ名>画面) に表示されます。

リモート リーフ スイッチのルーティング可能なサブネットの設定

1つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、リモート リーフ ノードが関連付けられているポッドのルーティング可能なサブネットを設定する必要があります。

-
- ステップ1** サイトの APIC GUI に直接ログインします。
- ステップ2** メニューバーから、[ファブリック (Fabric)] > [インベントリ (Inventory)] を選択します。
- ステップ3** [ナビゲーション (Navigation)] ウィンドウで、[ポッドファブリックセットアップポリシー (Pod Fabric Setup Policy)] をクリックします。
- ステップ4** メインペインで、サブネットを設定するポッドをダブルクリックします。
- ステップ5** ルーティング可能なサブネットエリアで、+ 記号をクリックしてサブネットを追加します。
- ステップ6** IPアドレスと予約アドレスの数を入力し、状態をアクティブまたは非アクティブに設定してから、[更新 (Update)] をクリックしてサブネットを保存します。
- ルーティング可能なサブネットを設定する場合は、/22~/29の範囲のネットマスクを指定する必要があります。
- ステップ7** [送信 (Submit)] をクリックして設定を保存します。
-

リモートリーフスイッチの直接通信の有効化

1つ以上のリモートリーフスイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、そのサイトに対して直接リモートリーフ通信を設定する必要があります。リモートリーフ直接通信機能に関する追加情報については、Cisco APIC レイヤ3ネットワークコンフィギュレーションガイドを参照してください。ここでは、Multi-Site との統合に固有の手順とガイドラインの概要を説明します。



-
- (注) リモートリーフスイッチの直接通信を有効にすると、スイッチは新しいモードでのみ機能します。
-

-
- ステップ1** サイトの APIC に直接ログインします。
- ステップ2** リモートリーフスイッチの直接トラフィック転送を有効にします。
- メニューバーから、[システム (System)] > [システムの設定 (System Settings)] に移動します。
 - 左側のサイドバーのメニューから [ファブリック全体の設定 (Fabric Wide Setting)] を選択します。
 - [リモートリーフ直接トラフィック転送 (Enable Remote Leaf Direct Traffic Forwarding)] チェックボックスをオンにします。
- (注) 有効にした後は、このオプションを無効にすることはできません。
- [送信 (Submit)] をクリックして変更を保存します。
-

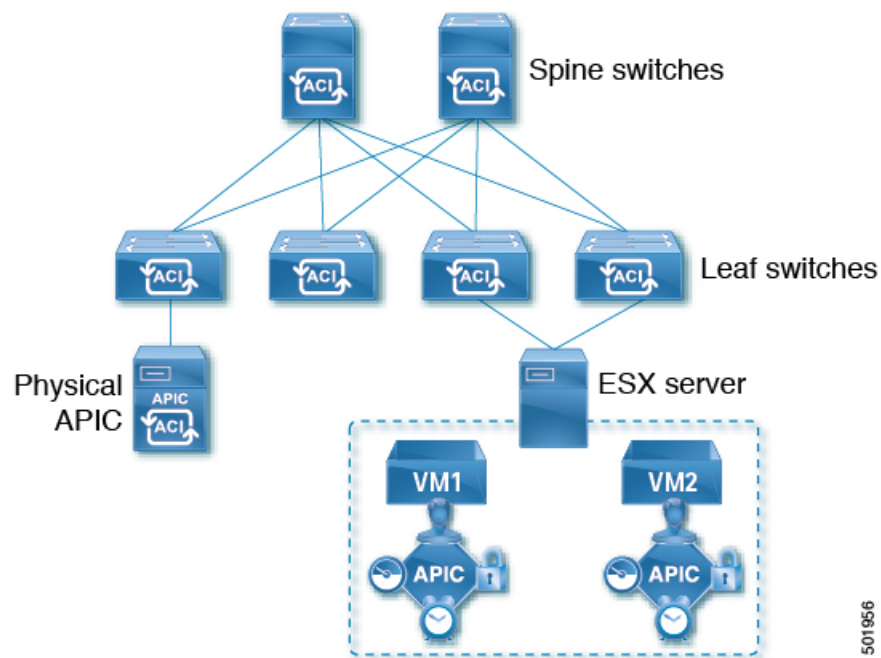
Cisco Mini ACI ファブリック

Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプ of ファブリックの導入と設定に関する詳細情報は、『[Cisco Mini ACI ファブリックおよび仮想 APIC](#)』に記述されています。

Cisco ACI リリース 4.0(1) では、小規模導入向けに Mini ACI ファブリックが導入されました。Mini ACI ファブリックは、仮想マシンで実行される1つの物理 APIC と2つの仮想 APIC (vAPIC) で構成される Cisco APIC クラスタで動作します。これにより、APIC クラスタの物理的なフットプリントとコストが削減され、ACI ファブリックを、物理的な設置面積や初期コストのために、フルスケールの ACI インストールが実用的でないような、ラックスペースや初期予算が限られたシナリオ (コロケーション施設やシングルルームデータセンターなど) に導入できるようになります。

次の図に、物理 APIC と2つの仮想 APIC (vAPIC) を備えたミニ Cisco ACI ファブリックの例を示します。

図 14: Cisco Mini ACI ファブリック



501956



第 12 章

サイトの追加と削除

- [Cisco NDO と APIC の相互運用性のサポート \(145 ページ\)](#)
- [Cisco ACI サイトの追加 \(147 ページ\)](#)
- [サイトの削除 \(150 ページ\)](#)
- [ファブリック コントローラへの相互起動 \(151 ページ\)](#)

Cisco NDO と APIC の相互運用性のサポート

Cisco Nexus Dashboard Orchestrator (NDO) では、すべてのサイトで特定のバージョンの APIC を実行する必要はありません。各サイトの APIC クラスタと NDO 自体は、Nexus Dashboard Orchestrator サービスがインストールされている Nexus ダッシュボードにファブリックをオンボードできる限り、相互に独立してアップグレードし、混合動作モードで実行することができます。そのため、常に Nexus Dashboard Orchestrator の最新リリースにアップグレードしておくことをお勧めします。

ただし、1つまたは複数のサイトで APIC クラスタをアップグレードする前に NDO をアップグレードすると、新しい NDO の機能の一部が、以前の APIC リリースでまだサポートされていないという状況が生じ得ることに注意してください。この場合、各テンプレートでチェックが実行され、すべての設定済みオプションがターゲットサイトでサポートされていることを確認します。

このチェックは、テンプレートを保存するか、テンプレートを展開するときに行われます。テンプレートがすでにサイトに割り当てられている場合、サポートされていない設定オプションは保存されません。テンプレートがまだ割り当てられていない場合は、サイトに割り当てることができますが、サイトがサポートしていない設定が含まれている場合は、スキーマを保存したり展開したりすることはできません。

サポートされていない設定が検出されると、エラーメッセージが表示されます。例: この APIC サイトバージョン<site version>は、NDO ではサポートされていません。この<feature>に必要な最小バージョンは<required-version>以降です。

次の表に、各機能と、それぞれに必要な最小限の APIC リリースを示します。



(注) 次の機能の一部は、以前の Cisco APIC リリースでサポートされていますが、Nexus ダッシュボードにオンボードし、このリリースの Nexus Dashboard Orchestrator で管理できる最も古いリリースは、リリース 4.2(4) です。

機能	最小バージョン
ACI マルチポッドのサポート	リリース 4.2(4)
サービス グラフ (L4 ~ L7 サービス)	リリース 4.2(4)
外部 EPG	リリース 4.2(4)
ACI 仮想エッジ VMM のサポート	リリース 4.2(4)
DHCP Support	リリース 4.2(4)
整合性チェッカー	リリース 4.2(4)
vzAny	リリース 4.2(4)
ホストベースのルーティング	リリース 4.2(4)
CloudSec 暗号化	リリース 4.2(4)
レイヤ 3 マルチキャスト	リリース 4.2(4)
OSPF の MD5 認証	リリース 4.2(4)
EPG 優先グループ	リリース 4.2(4)
サイト内 L3Out	リリース 4.2(4)
QoS の優先順位	リリース 4.2(4)
コントラクト QoS 優先順位	リリース 4.2(4)
シングルサインオン (SSO)	リリース 5.0(1)
マルチキャストランデブーポイント (RP) のサポート	リリース 5.0(1)
AWS および Azure サイトのトランジットゲートウェイ (TGW) サポート	リリース 5.0(1)
SR-MPLS サポート	リリース 5.0(1)
クラウド ロードバランサ 高可用性ポート	リリース 5.0(1)

機能	最小バージョン
UDR を使用したサービスグラフ (L4-L7 サービス)	Release 5.0(2)
クラウドでのサードパーティデバイスのサポート	Release 5.0(2)
クラウドロードバランサのターゲット接続モード機能	Release 5.1(1)
Express Route 経由で到達可能な非 ACI ネットワークの Azure でのセキュリティおよびサービス挿入サポート	Release 5.1(1)
CSR プライベート IP サポート	Release 5.1(1)
Azure のクラウドネイティブ サービスの ACI ポリシー モデルと自動化の拡張	Release 5.1(1)
Azure の単一 VNET 内での複数の VRF サポートによる柔軟なセグメンテーション	Release 5.1(1)
Azure PaaS およびサードパーティ サービスのプライベート リンク自動化	Release 5.1(1)
ACI-CNI を使用した Azure での OpenShift 4.3 IPI	Release 5.1(1)
クラウド サイト アンダーレイ の設定	リリース 5.2(1)

Cisco ACI サイトの追加

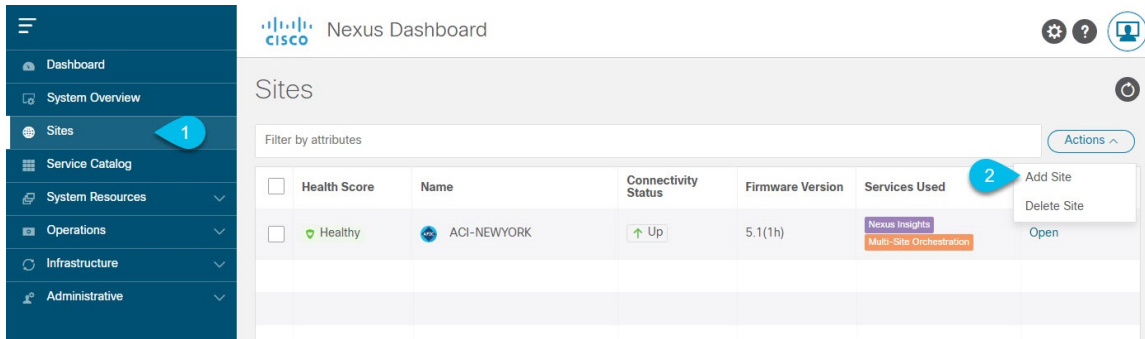
ここでは、Nexus Dashboard GUI を使用して Cisco APIC または Cloud APIC サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

始める前に

- この章の前のセクションで説明したように、オンプレミスの ACI サイトを追加する際には、各サイトの APIC でサイト固有の構成を完了している必要があります。
- 追加するサイトがリリース 4.2(4) 以降を実行していることを確認する必要があります。

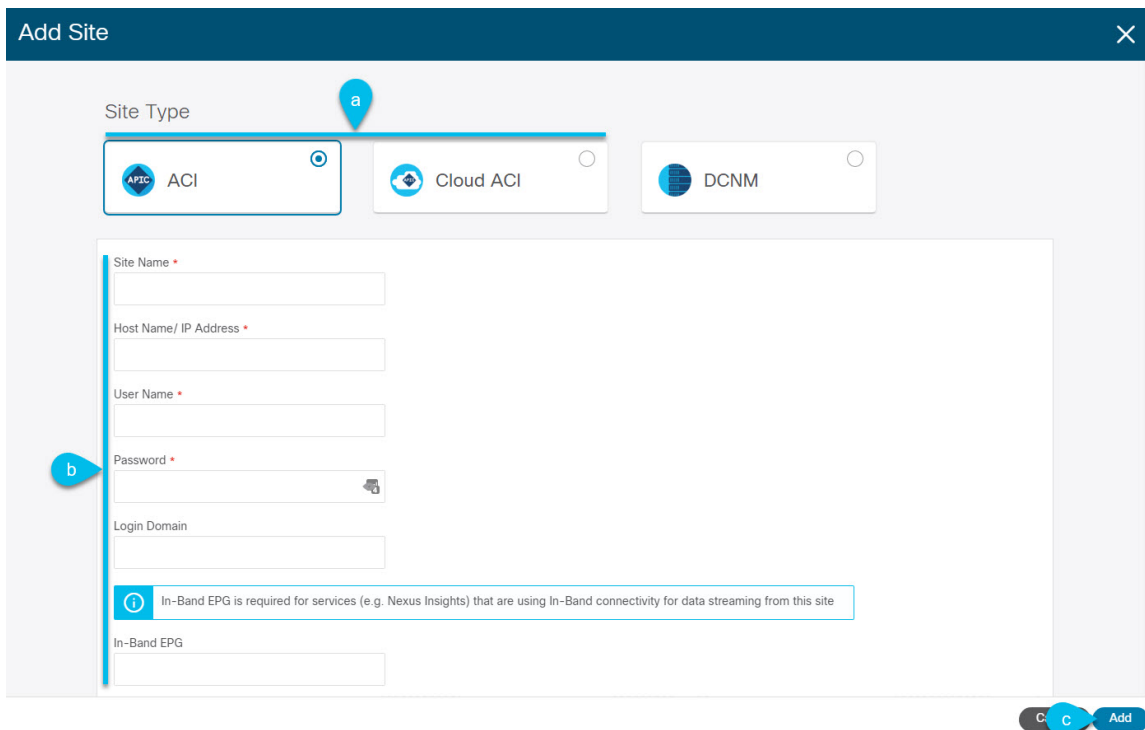
ステップ 1 Nexus ダッシュボード GUI にログインします。

ステップ 2 新サイトを追加します。



- a) 左のナビゲーションメニューから [サイト (Sites)] を選択します。
- b) メインペインの右上にある [アクション (Actions)] > [サイトの追加 (Add Site)] をクリックします。

ステップ 3 サイト情報を入力します。



- a) [サイトのタイプ (Site Type)] で、追加する ACI ファブリックのタイプに応じて [ACI] または [クラウド ACI (Cloud ACI)] を選択します。
- b) コントローラ情報を入力します。

- ACI ファブリックを現在管理している APIC コントローラについて、[ホスト名/IP アドレス (Host Name/IP Address)]、[ユーザー名 (User Name)]、および [パスワード (Password)] を入力する必要があります。用です。

(注) APIC ファブリックでは、Nexus Dashboard Orchestrator サービスのみでサイトを使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Nexus Dashboard Insights でもサイトを使用する場合は、インバンド IP アドレスを指定する必要があります。

- Cisco APIC によって管理されるオンプレミス ACI サイトの場合、このサイトを Nexus Insights などのデイ 2 オペレーション アプリケーションで使用する場合は、追加する Nexus ダッシュボードをファブリックに接続するために使用する **インバンド EPG** 名も指定する必要があります。それ以外の場合、このサイトを Nexus Dashboard Orchestrator でのみ使用する場合は、このフィールドを空白のままにすることができます。
- クラウド ACI サイトの場合、プロキシ経由でクラウドサイトに到達できる場合は、**プロキシを有効にします**。

プロキシは、Nexus Dashboard のクラスタ設定ですでに設定されている必要があります。管理ネットワーク経由でプロキシに到達できる場合は、プロキシ IP アドレス用のスタティック管理ネットワークルートも追加する必要があります。プロキシとルートの構成の詳細については、お使いのリリースの [Nexus Dashboard ユーザー ガイド](#) を参照してください。

- c) **[追加 (Add)]** をクリックして、サイトの追加を終了します。

この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

ステップ 4 他のサイトに対して上記の手順を繰り返します。

ステップ 5 Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** から、Nexus Dashboard Orchestrator サービスを開きます。

Nexus ダッシュボード ユーザーのクレデンシアルを使用して自動的にログインします。

ステップ 6 Nexus Dashboard Orchestrator GUI で、サイトを管理します。

Health	Name	Type	Templates	State	Controller URL
N/A	Fabric1	DCNM	0	Unmanaged	https://10.23.234.161:4...
N/A	Fabric2 Site ID: 65002	DCNM	0	Unmanaged	https://10.23.234.159:4...
N/A	Fabric3 Site ID: 65003	DCNM	0	Managed	https://10.23.234.159:4...

- a) 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]** を選択します。
- b) メインペインで、NDO で管理する各ファブリックの **[状態 (State)]** を **[非管理対象 (Unmanaged)]** から **[管理対象 (Managed)]** に変更します。

サイトの削除

ここでは、Nexus Dashboard Orchestrator GUI を使用して 1 つ以上のサイトのサイト管理を無効にする方法について説明します。サイトは Nexus ダッシュボードに残ります。

始める前に

削除するサイトに関連付けられているすべてのテンプレートが展開されていないことを確認する必要があります。

ステップ 1 Nexus Dashboard Orchestrator GUI を開きます。

Nexus ダッシュボードの**サービスカタログ**から NDO サービスを開きます。Nexus ダッシュボードユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 サイトのアンダーレイ設定を削除します。

- 左側のナビゲーションメニューで、**[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infra Configuration)]** を選択します。
- メイン ペインにある **[インフラの設定 (Configure Infra)]** をクリックします。
- 左側のサイドバーで、管理対象から外すサイトを選択します。
- 右側のバーの **[オーバーレイの設定 (Overlay Configuration)]** タブで、**[Multi-Site]** ノブを無効にします。
- 右側のサイドバーで、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択します。
- サイトからすべてのアンダーレイ設定を削除します。
- [展開 (Deploy)]** をクリックして、アンダーレイとオーバーレイの設定変更をサイトに展開します。

ステップ 3 Nexus Dashboard Orchestrator GUI で、サイトを無効にします。

- 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)] > [サイト (Sites)]** を選択します。
- メイン ペインで、NDO で管理する各ファブリックの **[状態 (State)]** を **[管理対象 (Managed)]** から **[非管理対象 (Unmanaged)]** に変更します。

(注) サイトが 1 つ以上の展開済みテンプレートに関連付けられている場合、それらのテンプレートを展開解除するまで、その状態を **[非管理対象 (Unmanaged)]** に変更することはできません。

ステップ 4 Nexus ダッシュボードからサイトを削除します。

このサイトを管理したり、他のアプリケーションで使用したりする必要がなくなった場合は、Nexus ダッシュボードからもサイトを削除できます。

(注) この時点で、このサイトは、Nexus Dashboard クラスタにインストールされているどのアプリケーションでも使用されていないことに注意してください。

- Nexus ダッシュボード GUI の左側のナビゲーションメニューから、**[サイト (Sites)]** を選択します。
- 削除するサイトを 1 つ以上選択します。
- メイン ペインの右上にある **[アクション (Actions)] > [サイトの削除 (Delete Site)]** をクリックします。

- d) サイトのログイン情報を入力し、**[OK]** をクリックします。
Nexus ダッシュボードからサイトが削除されます。

ファブリックコントローラへの相互起動

Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとに多数の設定オプションをサポートしています。追加の多くの設定オプションでは、ファブリックのコントローラに直接ログインする必要があります。

NDO の[インフラストラクチャ (**Infrastructure**)] > [サイト (**Sites**)]画面から特定のサイトコントローラの GUI にクロス起動するには、サイトの横にあるアクション (...) メニューを選択し、ユーザーインターフェイスで **[開く (Open)]** をクリックします。クロス起動は、ファブリックのアウトオブバンド (OOB) 管理 IP で動作することに注意してください。

Nexus Dashboard とファブリックで同じユーザが設定されている場合、Nexus Dashboard ユーザと同じログイン情報を使用して、ファブリックのコントローラに自動的にログインします。一貫性を保つために、Nexus ダッシュボードとファブリック全体で共通のユーザによるリモート認証を設定することを推奨します。



第 13 章

インフラ一般設定

- インフラ設定ダッシュボード (153 ページ)
- パーシャルメッシュサイト間接続 (154 ページ)
- インフラの設定: 一般設定 (155 ページ)

インフラ設定ダッシュボード

[インフラ設定 (Infra Configuration)] ページには、Nexus Dashboard Orchestrator 展開環境のすべてのサイトとサイト間接続の概要が表示されます。

図 15: インフラ設定の概要

The screenshot displays the 'Site Connectivity' page in the Cisco Nexus Dashboard Orchestrator. The left-hand navigation menu is expanded to show 'Site Connectivity'. The main content area is titled 'Site Connectivity' and features a 'Configure' button. Below this, there are three main sections: 'General Settings', 'scale-ms11', and 'Azsite1'. The 'General Settings' section includes BGP Peering Type (full-mesh), Keep Alive Interval (60s), Hold Interval (180s), BGP TTL Between Peers (16), Stale Interval (300s), Graceful Restart (On), and Maximum AS Limit (0). The 'scale-ms11' section shows 1 Pod and 1 Spine, with ACI Multi-Site (On), Cloudsec Encryption (On), APIC Site ID (254), BGP Autonomous Sys Number (511), OSPF Area ID (0), OSPF Area Type (regular), and Overlay Multicast TEP (11.11.11.10). The 'Azsite1' section shows 4 Regions, ACI Multi-Site (On), APIC Site ID (21), and BGP Autonomous Sys Number (65145). At the bottom, there is an 'Inter-Site Connections' table with tabs for 'Overlay Status' and 'Underlay Status'. The table shows one connection for 'onPrem2' with a deployment status of 'OK', an operational status of 'Fail', an overlay routing status of 'Fail', and a tunnel status of '4 up 0 down 4'. A 'Hide Connectivity Status' button is also visible.

1. **[全般設定 (General Settings)]** タイルには、BGP ピアリングタイプとその設定に関する情報が表示されます。
詳細については、次のセクションで説明します。
2. **[オンプレミス (On-Premises)]** タイルには、ポッドとスパインスイッチの数、OSPF 設定、およびオーバーレイ IP とともに、Multi-Site ドメインの一部であるすべてのオンプレミスサイトに関する情報が表示されます。
サイト内のポッドの数を表示する**[ポッド (Pods)]** タイルをクリックすると、各ポッドのオーバーレイユニキャスト TEP アドレスに関する情報を表示できます。
詳細については、[Cisco APIC サイトのインフラの設定 \(161 ページ\)](#) を参照してください。
3. **[クラウド (Cloud)]** タイルには、Multi-Site ドメインの一部であるすべてのクラウドサイトに関する情報と、リージョン数および基本的なサイト情報が表示されます。
詳細については、[Cisco Cloud APIC サイトのインフラの設定 \(169 ページ\)](#) を参照してください。
4. **[接続ステータスの表示]** をクリックして、特定のサイトのサイト間接続の詳細を表示できます。
5. **[構成]** ボタンを使用して、サイト間接続構成に移動できます。これについては、次のセクションで詳しく説明します。

次のセクションでは、全般的なファブリックインフラ設定を行うために必要な手順について説明します。ファブリック固有の要件と手順は、管理するファブリックの特定のタイプに基づいて、次の章で説明します。

インフラの設定を進める前に、前のセクションで説明したようにサイトを設定して追加する必要があります。

加えて、スパインスイッチの追加や削除、またはスパインノードIDの変更などのインフラストラクチャの変更には、一般的なインフラの設定手順の一部として、[サイト接続性情報の更新 \(161 ページ\)](#) に記載されているような、Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

パーシャルメッシュサイト間接続

Nexus Dashboard Orchestrator が管理するすべてのサイトから他のすべてのサイトへのサイト間接続を構成するフルメッシュ接続に加えて、このリリースではパーシャルメッシュ構成もサポートしています。パーシャルメッシュ構成では、他のサイトへのサイト間接続を持たないスタンドアロンモードでサイトを管理したり、サイト間構成をマルチサイトドメイン内の他のサイトのサブセットのみに制限したりできます。

Nexus Dashboard Orchestrator リリース 3.6(1) より前では、サイト間のサイト間接続が構成されていなくても、サイト間でテンプレートを拡張し、他のサイトに展開された他のテンプレートからポリシーを参照でき、それらのサイト間のサイト間接続が構成されていなくても、サイト間で動作しない意図したトラフィックフローが発生します。

リリース 3.6(1)以降、Orchestrator では、それらのサイト間のサイト間接続が適切に構成および展開されている場合にのみ、（他のサイトに展開されている）他のテンプレートからテンプレートとリモート参照ポリシーを 2 つ以上のサイト間で拡張できます。

次のセクションで説明するように、Cisco APIC および Cisco Cloud APIC サイトのサイトインフラストラクチャを構成する場合、サイトごとに、他のどのサイトインフラストラクチャ接続を確立するかを明示的に選択し、その構成情報のみを提供できます。

パーシャルメッシュ接続のガイドライン

パーシャルメッシュ接続を構成するときは、次のガイドラインを考慮してください。

- パーシャルメッシュ接続は、2つのクラウドサイト間、またはクラウドとオンプレミスのサイト間でサポートされています。

すべてのオンプレミス サイト間で完全なメッシュ接続が自動的に確立されます。

- パーシャルメッシュ接続は、BGP-EVPN または BGP-IPv4 プロトコルを使用してサポートされています。

ただし、テンプレートのストレッチは、BGP-EVPN プロトコルを使用して接続されているサイトに対してのみ許可されることに注意してください。BGP-IPv4 を使用して 2 つ以上のサイトを接続している場合、それらのサイトのいずれかに割り当てられたテンプレートは、1 つのサイトにのみ展開できます。

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。



- (注) 次の設定には、すべてのサイトに適用されるものと、特定のタイプのサイト（クラウド APIC サイトなど）に必要なものがあります。各サイト固有のサイトローカル設定に進む前に、インフラ一般設定で必要なすべての設定を完了していることを確認します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メインペインにある [構成 (Configure)] をクリックします。

ステップ 4 左側のサイドバーで、[全般設定 (General Settings)] を選択します。

ステップ 5 [コントロールプレーン設定 (Control Plane Configuration)] を指定します。

- a) [コントロールプレーン設定 (Control Plane Configuration)] タブを選択します。
- b) [BGP ピアリングタイプ (Bgp Peering Type)] を選択します。

- **full-mesh** : 各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。

[フルメッシュ] 構成では、Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパイン スイッチと DCNM 管理ファブリックのボーダー ゲートウェイを使用します。

- [route-reflector] : **route-reflector** オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルート リフレクタ ノードを使用すると、NDO によって管理されるすべてのサイト間で MP-BGP EVPN フルメッシュ隣接関係が作成されなくなります。

ACIファブリックの場合、[route-reflector] オプションは、同じ BGP ASN の一部であるファブリックに対してのみ有効です。

- c) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。
- デフォルト値を維持することを推奨します。
- d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。
- デフォルト値を維持することを推奨します。
- e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。
- デフォルト値を維持することを推奨します。
- f) **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。
- g) **[AS 上限 (Maximum AS Limit)]** を入力します。
- デフォルト値を維持することを推奨します。
- h) **[ピア間のBGP TTL (BGP TTL Between Peers)]** を入力します。
- デフォルト値を維持することを推奨します。
- i) **[OSPF エリア ID (OSPF Area ID)]** を入力します。
- クラウド APIC サイトがない場合、このフィールドは UI に表示されません。
- これは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス IPN ピ어링用のクラウドサイトで使用される OSPF エリア ID です。

ステップ 6 [IPN デバイス情報] を入力します。

オンプレミスとクラウドサイト間のサイト間接続を設定する予定がない場合は、この手順をスキップできます。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスサイトの設定画面で使用可能になる前に、ここで定義する必要があります。詳細は [インフラの設定: オンプレミス サイトの設定 \(162 ページ\)](#) を参照してください。

- a) **[デバイス (Devices)]** タブを選択します。

- b) **[IPN デバイスの追加 (Add IPN Device)]** をクリックします。
- c) IPN デバイスの **[名前 (Name)]** と **[IP アドレス (IP Address)]** を入力します。
指定した IP アドレスは、IPN デバイスの管理 IP アドレスではなく、クラウド APIC の CSR からのトンネルピアアドレスとして使用されます。
- d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
- e) 追加する IPN デバイスについて、この手順を繰り返します。

ステップ 7 **[外部 デバイス (External Devices)]** 情報を入力します。

クラウド APIC サイトがない場合、このタブは UI に表示されません。

Multi-Site ドメインにクラウド APIC サイトがない場合、またはクラウドサイトとブランチルータまたはその他の外部デバイス間の接続を設定する予定がない場合は、この手順をスキップできます。

次の手順では、クラウドサイトからの接続を設定するブランチルータまたは外部デバイスに関する情報を指定する方法について説明します。

- a) **[外部デバイス (External Devices)]** タブを選択します。
このタブは、Multi-Site ドメインに少なくとも 1 つのクラウドサイトがある場合にのみ使用できます。
- b) **[外部デバイスの追加 (Add External Device)]** をクリックします。
[外部デバイスの追加 (Add External Device)] ダイアログが開きます。
- c) デバイスの **[名前 (Name)]**、**[IP アドレス (IP Address)]**、および **[BGP 自律システム番号 (BGP Autonomous System Number)]** を入力します。
指定した IP アドレスは、デバイスの管理 IP アドレスではなく、クラウド APIC の CSR からのトンネルピアアドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。
- d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
- e) 追加する IPN デバイスについて、この手順を繰り返します。

すべての外部デバイスを追加したら、次の手順を完了して、IPSec トンネル サブネット プールにこれらのトンネルに割り当てられる内部 IP アドレスを指定します。

ステップ 8 **[IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)]** 情報を入力します。

クラウド APIC サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール** : クラウドサイトの CSR と他のサイト (クラウドまたはオンプレミス) 間の接続に使用されます。

これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバルサブネットプールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

1 つ以上のクラウドサイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネットプールを提供する必要があります。

- **サイト固有のサブネット プール** : クラウドサイトの CSR と外部デバイス間の接続に使用されます。これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウドサイトの IPsec トンネルで引き続き使用する場合です。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

名前付きサブネット プールを指定しない場合でも、クラウドサイトの CSR と外部デバイス間の接続を設定すると、外部サブネット プールが IP 割り当てに使用されます。

(注) 両方のサブネット プールの最小マスク長は /24 です。

1 つ以上の外部サブネット プールを追加するには :

- [IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)]** タブを選択します。
- [外部サブネット プール (External Subnet Pool)]** エリアで、**[+IP アドレスの追加 (+Add IP Address)]** をクリックして、1 つ以上の外部サブネット プールを追加します。

このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス接続に使用されるクラウドルータの IPsec トンネルインターフェイスとループバックに対処するために使用されます。

サブネットは、他のオンプレミス TEP プールと重複してはならず、0.xxx または 0.0.xxx で始まってはならず、/16 と /24 の間のネットワーク マスク (30.29.0.0/16 など) が必要です。

- チェックマーク アイコンをクリックして、サブネット情報を保存します。
- 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール (Site-Specific Subnet Pools)]** を追加するには :

- [IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)]** タブを選択します。
- [サイト固有のサブネット プール (Site-Specific Subnet Pools)]** エリアで、**[+IP アドレスの追加 (+Add IP Address)]** をクリックして、1 つ以上の外部サブネット プールを追加します。

[名前付きサブネット プールの追加 (Add Named Subnet Pool)] ダイアログが開きます。

- サブネットの **[名前 (Name)]** を入力します。
後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。
- [+IP アドレスの追加 (+Add IP Address)]** をクリックして、1 つ以上のサブネット プールを追加します。
サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。
- チェックマーク アイコンをクリックして、サブネット情報を保存します。
同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。
- [保存 (Save)]** をクリックして、名前付きサブネット プールを保存します。
- 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（オンプレミスACI、クラウドACI、またはオンプレミスファブリック）に基づいて、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。



第 14 章

Cisco APIC サイトのインフラの設定

- [サイト接続性情報の更新 \(161 ページ\)](#)
- [インフラの設定: オンプレミス サイトの設定 \(162 ページ\)](#)
- [インフラの設定: ポッドの設定 \(165 ページ\)](#)
- [インフラの設定: スパイン スイッチ \(165 ページ\)](#)

サイト接続性情報の更新

スパインの追加や削除、またはスパイン ノードの ID 変更などのインフラストラクチャへの変更が加えられた場合、Multi-Site ファブリック接続サイトの更新が必要になります。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。

ステップ 4 左側のペインの [サイト (Sites)] の下で、特定のサイトを選択します。

ステップ 5 メイン ウィンドウで、APIC からファブリック情報を取得するために [更新 (Refresh)] ボタンをクリックします。

ステップ 6 (オプション) オンプレミス サイトの場合、廃止されたスパイン スイッチ ノードの設定を削除する場合は、[確認 (Confirmation)] ダイアログで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有効にすると、現在使用されていないスパイン スイッチのすべての設定情報がデータベースから削除されます。

ステップ 7 最後に、[はい (Yes)] をクリックして確認し、接続情報をロードします。

これにより、新しいスパインや削除されたスパインを検出し、すべてのサイトに関連したファブリックの接続を APIC からインポートし直します。

インフラの設定: オンプレミス サイトの設定

ここでは、オンプレミスサイトにサイト固有のインフラ設定を構成する方法について説明します。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。
- ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。
- ステップ 4 左側のペインの [サイト (Sites)] の下で、特定のオンプレミス サイトを選択します。
- ステップ 5 [サイト間接続 (Inter-Site Connectivity)] 情報を入力します。
 - a) 右側の <サイト (Site)> [設定 (Settings)] ペインで、[マルチサイト (Multi-Site)] ノブを有効にします。これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。
 - b) (オプション n) [CloudSec 暗号化 (CloudSec Encryption)] ノブを有効にして、サイトを暗号化します。CloudSec 暗号化は、サイト間トラフィックの暗号化機能を提供します。この機能の詳細については、[Cisco Multi-Site Configuration Guide](#) の「Infrastructure Management」の章を参照してください。
 - c) [オーバーレイ マルチキャスト TEP (Overlay Multicast TEP)] を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、単一のポッドまたはマルチポッドファブリックであるかどうかには関わりなく、同じファブリックの一部であるすべてのスパイン スイッチに展開されます。

このアドレスは、元のファブリックのインフラ TEP プールのアドレス空間または 0.x.x.x の範囲から取得することはできません。
 - d) [BGP 自律システム番号 (BGP Autonomous System Number)] を指定します。
 - e) (オプション) [BGP パスワード (BGP Password)] を指定します。
 - f) [OSPF エリア ID (OSPF Area ID)] を入力します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、[インフラの設定: スパイン スイッチ \(165 ページ\)](#) で説明されているように、ポート レベルで行われます。
 - g) ドロップダウン メニューから [OSPF エリア タイプ (OSPF Area Type)] を選択します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、[インフラの設定: スパイン スイッチ \(165 ページ\)](#) で説明されているように、ポート レベルで行われます。

OSPF エリアタイプは、次のいずれかになります。

 - nssa
 - regular

h) サイトの OSPF ポリシーを設定します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、[インフラの設定: スパインスイッチ \(165 ページ\)](#) で説明されているように、ポート レベルで行われます。

既存のポリシー (たとえば `msc-ospf-policy-default`) をクリックして修正することも、**[+ ポリシー追加(+Add Policy)]** をクリックして新しい OSPF ポリシーを追加することもできます。それから、**[ポリシーの追加/更新(Add/Update Policy)]** ウィンドウで、以下を指定します。

- **[ポリシー名 (Policy Name)]** フィールドにポリシー名を入力します。
- **[(ネットワーク タイプ (Network Type))]** フィールドで、**[ブロードキャスト (broadcast)]**、**[ポイントツーポイント (point-to-point)]**、または **[未指定 (unspecified)]** のいずれかを選択します。
デフォルトは **[ブロードキャスト (broadcast)]** です。
- **[優先順位 (Priority)]** フィールドに、優先順位番号を入力します。
デフォルトは 1 です。
- **[インターフェイスのコスト (Cost of Interface)]** フィールドに、インターフェイスのコストを入力します。
デフォルト値は 0 です。
- **[インターフェイスコントロール(Interface Controls)]** ドロップダウンメニューで、以下のいずれかを選択します。
 - **アドバタイズサブネット (advertise-subnet)**
 - **BFD (bfd)**
 - **MTU 無視 (mtu-ignore)**
 - **受動的参加 (passive-participation)**
- **[Hello 間隔 (秒) (Hello Interval (Seconds))]** フィールドに、hello 間隔を秒単位で入力します。
デフォルト値は 10 です。
- **[Dead 間隔 (秒) (Dead Interval (Seconds))]** フィールドに、dead 間隔を秒単位で入力します。
デフォルト値は 40 です。
- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。
デフォルト値は 5 です。
- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。
デフォルトは 1 です。

i) (オプション) **[外部ルート ドメイン (External Routed Domain)]** ドロップダウンから、使用するドメインを選択します。

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。使用している APIC リリースに固有の詳細については、『[Cisco APIC Layer 3 Networking Configuration Guide](#)』を参照してください。

- j) (オプション) サイトの **[SDA 接続 (SDA Connectivity)]** を有効にします。

サイトが SDA ネットワークに接続されている場合は、**SDA 接続** ノブを有効にして、**外部ルーテッドドメイン**、**VLAN プール**、および **VRF Lite IP プール範囲** の情報を提供します。

サイトの SDA 接続を有効にする場合は、『[Cisco Multi-Site Configuration Guide for ACI Fabrics](#)』の「SDA 使用例」の章で説明されている追加構成を行う必要があります。

- k) (オプション) サイトの **[SR-MPLS 接続 (SR-MPLS Connectivity)]** を有効にします。

サイトが MPLS ネットワークを介して接続されている場合には、**[SR-MPLS 接続性 (SR-MPLS Connectivity)]** ノブを有効にして、セグメントルーティング グローバルブロック (SRGB) の範囲を指定します。

セグメントルーティング グローバルブロック (SRGB) は、ラベルスイッチングデータベース (LSD) でセグメントルーティング (SR) 用に予約されているラベル値の範囲です。これらの値は SR 対応ノードへのセグメント識別子 (SID) として割り当てられ、ドメイン全体でグローバルな意味を持ちます。

デフォルトの範囲は 16000 ~ 23999 です。

サイトの MPLS 接続を有効にする場合は、『[Cisco Multi-Site Configuration Guide for ACI Fabrics](#)』の「Sites Connected via SR-MPLS」の章で説明されている追加設定を行う必要があります。

ステップ 6 オンプレミスとクラウドサイト間のサイト間接続を設定します。

オンプレミスサイトとクラウドサイトの間にはサイト間接続を作成する必要がない場合（たとえば、導入にクラウドのみまたはオンプレミスサイトのみが含まれる場合）は、この手順をスキップします。

オンプレミスとクラウドサイト間のアンダーレイ接続を設定する場合は、クラウド APIC の CSR がトンネルを確立する IPN デバイスの IP アドレスを指定し、クラウドサイトのインフラ設定を行う必要があります。

- a) **[+ IPN デバイスの追加 (+ Add IPN Device)]** をクリックして、IPN デバイスを指定します。
 b) ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPN デバイスは、**[一般設定 (General Settings)] > [IPN デバイス (IPN Devices)]** リストですでに定義されている必要があります。 [インフラの設定: 一般設定 \(155 ページ\)](#) を参照してください。

- c) クラウドサイトのサイト間接続を設定します。

クラウドサイトからこのオンプレミスサイトへの以前に設定された接続はすべてここに表示されますが、追加の設定は、[Cisco Cloud APIC サイトのインフラの設定 \(169 ページ\)](#) の説明に従ってクラウドサイト側から行う必要があります。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。[インフラ設定の展開 \(173 ページ\)](#) の説明に従って、設定を展開する必要があります。

インフラの設定: ポッドの設定

このセクションでは、各サイトでポッド固有の設定を行う方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メインペインの右上にある [構成 (Configure)] をクリックします。

ステップ 4 左側のペインの [サイト (Sites)] の下で、特定のサイトを選択します。

ステップ 5 メイン ウィンドウで、ポッドを選択します。

ステップ 6 右の [ポッドのプロパティ (Pod Properties)] ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

この IP アドレスは、同じポッドの一部であるすべてのスパインスイッチに展開され、レイヤ 2 およびレイヤ 3 ユニキャスト通信の VXLAN カプセル化トラフィックの送信と受信に使用されます。

ステップ 7 [+ TEP プールの追加 (+Add TEP Pool)] をクリックして、ルーティング可能な TEP プールを追加します。

外部ルーティング可能な TEP プールは、IPN 経由でルーティング可能な IP アドレスのセットを APIC ノード、スパインスイッチ、および境界リーフ ノードに割り当てるために使用されます。これは、Multi-Site アーキテクチャを有効にするために必要です。

以前に APIC でファブリックに割り当てられた外部 TEP プールは、ファブリックが Multi-Site ドメインに追加されると、NDO によって自動的に継承され、GUI に表示されます。

ステップ 8 サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパインスイッチ

このセクションでは、Cisco Multi-Site のために各サイトのスパインスイッチを設定する方法について説明します。スパインスイッチを設定する場合、各サイトのスパインと ISN 間の接続を設定することで、Multi-Site ドメイン内のサイト間のアンダーレイ接続を効果的に確立できます。

リリース 3.5(1) より前は、OSPF プロトコルを使用してアンダーレイ接続が確立されていました。一方、このリリースでは、OSPF、BGP (IPv4 のみ)、または混合プロトコルを使用できます。混合とは、一部のサイトではサイト間アンダーレイ接続に OSPF を使用し、一部のサイトでは BGP を使用することです。両方ではなく OSPF または BGP のいずれかを設定すること

を推奨します。両方のプロトコルを設定した場合には、BGPが優先され、OSPFはルートテーブルにインストールされません。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。

ステップ 4 左側のペインの [サイト (Sites)] の下で、特定のオンプレミス サイトを選択します。

ステップ 5 メイン ペインで、ポッド内のスパイン スイッチを選択します。

ステップ 6 右側の [<スパイン> 設定 (Settings)] ペインで、[+ ポート追加 (Add Port)] をクリックします。

ステップ 7 [ポートの追加 (Add Port)] ウィンドウで、アンダーレイの接続情報を入力します。

IPN 接続用に APIC で直接設定されているポートがインポートされ、リストに表示されます。NDO から設定する新しいポートについては、次の手順を使用します。

a) 次の一般情報を指定します。

- **[イーサネット ポート ID (Ethernet Port ID)]** フィールドに、ポート ID、たとえば 1/29 を入力します。

これは、IPN への接続に使用されるインターフェイスです。

- **[IP アドレス (IP Address)]** フィールドに、IP アドレス/ネットマスクを入力します。

Orchestrator によって、指定された IP アドレスを持ち、指定されたポートを使用する、VLAN 4 のサブインターフェイスが作成されます。

- **[MTU]** フィールドに、サーバの MTU を入力します。MTU を 9150B に設定する継承を指定するか、576 ~ 9000 の値を選択します。

スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。

ステップ 8 アンダーレイ プロトコルを選択します。

a) アンダーレイ接続に OSPF プロトコルを使用する場合は、[OSPF] を設定します。

代わりに、アンダーレイ接続に BGP プロトコルを使用する場合は、この部分をスキップし、次のサブステップで必要な情報を入力します。

- **[OSPF]** を [有効 (Enabled)] に設定します。

OSPF 設定が使用可能になります。

- **[OSPF ポリシー (OSPF Policy)]** ドロップダウンで、[インフラの設定: オンプレミス サイトの設定 \(162 ページ\)](#) で設定したスイッチの OSPF ポリシーを選択します。

OSPF ポリシーの OSPF 設定は、IPN 側と一致させる必要があります。

- **[OSPF 認証 (OSPF Authentication)]** では、[なし (none)] または以下のいずれかを選択します。

- MD5

- Simple

- **[BGP]** を [無効 (Disabled)] に設定します。

b) アンダーレイ接続に BGP プロトコルを使用する場合は、**[BGP]** を有効にします。

アンダーレイ接続に OSPF プロトコルを使用しており、前のサブステップですでに設定している場合は、この部分をスキップします。

(注) 次の場合、BGP IPv4 アンダーレイはサポートされません。

- マルチサイト ドメインに 1 つ以上の Cloud APIC サイトが含まれている場合、オンプレミスからオンプレミスおよびオンプレミスからクラウドサイトの両方のサイト間アンダーレイ接続に OSPF プロトコルを使用する必要があります。
- いずれかのファブリックの WAN 接続に GOLF (ファブリック WAN のレイヤ 3 EVPN サービス) を使用している場合。

上記の場合、スパインに展開された Infra L3Out で OSPF を使用する必要があります。

- **[OSPF]** を [無効 (Disabled)] に設定します。

両方ではなく OSPF または BGP のいずれかを設定することを推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルート テーブルにインストールされません。ISN デバイスとの EBGW 隣接関係だけがサポートされるからです。

- **[BGP]** を [有効 (Enabled)] に設定します。

BGP 設定が使用可能になります。

- **[ピア IP (Peer IP)]** フィールドに、このポートの BGP ネイバーの IP アドレスを入力します。

BGP アンダーレイ接続では、IPv4 IP アドレスのみがサポートされます。

- **[ピア AS 番号 (Peer AS Number)]** フィールドに、BGP ネイバーの自律システム (AS) 番号を入力します。

このリリースでは、ISN デバイスとの EBGW 隣接関係のみがサポートされます。

- **[BGP パスワード (BGP Password)]** フィールドに、BGP ピア パスワードを入力します。

- 必要に応じて追加のオプションを指定します。

- [双方向フォワーディング検出 (Bidirectional Forwarding Detection)] : 双方向フォワーディング検出 (BFD) プロトコルを有効にして、このポートと IPN デバイスの物理リンクの障害を検出します。
- [管理状態 (Admin State)] : ポートの管理状態を有効に設定します。

ステップ 9 IPN に接続するすべてのスパイン スイッチおよびポートに対してこの手順を繰り返します。



第 15 章

Cisco Cloud APIC サイトのインフラの設定

- [クラウド サイト接続性情報の更新 \(169 ページ\)](#)
- [インフラの設定: クラウドサイトの設定 \(170 ページ\)](#)

クラウド サイト接続性情報の更新

CSR やリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。
- ステップ 3** メインペインの右上にある [構成 (Configure)] をクリックします。
- ステップ 4** 左側のペインの [サイト (Sites)] の下で、特定のサイトを選択します。
- ステップ 5** メインウィンドウで [更新 (Refresh)] ボタンをクリックして、新規または変更された CSR およびリージョンを検出します。
- ステップ 6** 最後に、[はい (Yes)] をクリックして確認し、接続情報をロードします。
これにより、新規または削除された CSR およびリージョンが検出されます。
- ステップ 7** [導入 (Deploy)] をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。
クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ設定を展開して、そのクラウドサイトへのアンダーレイ接続がある他のサイトが更新された設定を取得する必要があります。

インフラの設定:クラウドサイトの設定

ここでは、クラウド APIC サイトにサイト固有のインフラ設定を構成する方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。

ステップ 4 左側のペインの [サイト (Sites)] の下で、特定のクラウドサイトを選択します。

ステップ 5 [サイト間接続 (Inter-Site Connectivity)] 情報を入力します。

- a) 右側の [<Site> 設定 (Settings)] ペインで、[サイト間接続 (Inter-Site Connectivity)] タブを選択します。
- b) マルチサイト ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

- c) (オプション) [BGP パスワード (BGP Password)] を指定します。

ステップ 6 サイト固有の [サイト間接続 (Inter-Site Connectivity)] 情報を入力します。

- a) クラウドサイトの右側のプロパティ サイドバーで、[サイトの追加] をクリックします。

[サイトの追加 (Add Site)] ウィンドウが表示されます。

- b) [サイトへの接続] で、[サイトの選択] をクリックし、構成しているサイト (たとえば、site1) からの接続を確立するサイト (たとえば、site2) を選択します。

リモートサイトを選択すると、[サイトの追加] ウィンドウが更新され、両方向の接続が反映されます: **Site1 > Site2** および **Site2 > Site1**。

- c) [サイト1 (Site1)] > [サイト2 (Site2)] エリアで、[接続タイプ (Connection Type)] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

- [パブリックインターネット (Public Internet)] : 2つのサイト間の接続は、インターネットを介して確立されます。
このタイプは、任意の2つのクラウドサイト間、またはクラウドサイトとオンプレミスサイト間でサポートされます。
- [プライベート接続 (Private Connection)] : 2つのサイト間のプライベート接続を使用して接続が確立されます。
このタイプは、クラウドサイトとオンプレミスサイトの間でサポートされます。
- [クラウド バックボーン (Cloud Backbone)] : クラウドバックボーンを使用して接続が確立されます。

このタイプは、Azure-to-AzureやAWS-to-AWSなど、同じタイプの2つのクラウドサイト間でサポートされます。

複数のタイプのサイト（オンプレミス、AWS、Azure）がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

- d) これら2つのサイト間の接続に使用する**プロトコル**を選択します。

BGP-EVPN 接続を使用している場合は、オプションで **IPSec** を有効にして、使用する **Internet Key Exchange (IKE)** プロトコルのバージョンを選択できます。構成に応じて、**IKEv1** (バージョン 1) または **IKEv2** (バージョン 1) です。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- クラウド バックボーン接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

代わりに **BGP-IPv4** 接続を使用する場合は、構成しているクラウドサイトからのルート リーク構成に使用される外部 VRF を提供する必要があります。

Site1 > Site2 の接続情報が提供された後、**Site2 > Site1** 領域は、反対方向の接続情報を反映します。

- e) **[保存 (Save)]** をクリックして、設定を保存します。

site1 から site2 への接続情報を保存すると、site2 から site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、右側のサイドバーにある **[サイト間接続 (Inter-site Connectivity)]** 情報を選択することで確認できます。

- f) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

site1 から site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、site1 から site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

ステップ 7 [外部接続 (External Connectivity)] 情報を入力します。

NDOによって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。

外部接続のユースケースの詳細な説明は、「[Nexus Dashboard Orchestrator を使用したクラウド CSR からの外部接続の設定](#)」ドキュメントで入手できます。

- a) 右側の **[<Site> 設定 (Settings)]** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

- c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、クラウドルートをリークするために使用される VRF です。**[リージョン (Regions)]** セクションには、この設定を適用する CSR を含むクラウドリージョンが表示されます。

- d) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]**>**[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、**インフラの設定: 一般設定 (155 ページ)** の説明に従ってすでに定義されている必要があります。

- e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウドサイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。
- f) (任意) **[トンネルサブネットプール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネットプールのいずれかを選択します。

名前付きサブネットプールは、クラウドサイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで**名前付きサブネットプール**を指定しない場合、**外部サブネットプール**が IP 割り当てに使用されます。

外部デバイス接続用の専用サブネットプールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを NDO およびクラウドサイトの IPSec トンネルに引き続き使用する場合に役立ちます。

この接続に特定のサブネットプールを提供する場合は、**インフラの設定: 一般設定 (155 ページ)** の説明に従って作成済みである必要があります。

- g) (オプション) **[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタムキーを入力します。
- h) 必要に応じて、同じ外部接続 (同じ VRF) に対して追加する外部デバイスについて、前のサブステップを繰り返します。
- i) 必要に応じて、追加の外部接続 (異なる VRF) に対してこの手順を繰り返します。

CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。**インフラ設定の展開 (173 ページ)** の説明に従って、設定を展開する必要があります。



第 16 章

ACI サイト向けのインフラ設定の展開

- [インフラ設定の展開](#) (173 ページ)
- [オンプレミスとクラウド サイト間の接続の有効化](#) (174 ページ)

インフラ設定の展開

ここでは、各 APIC サイトにインフラ設定を展開する方法について説明します。

ステップ 1 メインペインの右上にある **[展開 (deploy)]** をクリックして、設定を展開します。

オンプレミスまたはクラウドサイトのみを設定した場合は、**[展開 (Deploy)]** をクリックしてインフラ設定を展開します。

ただし、オンプレミスとクラウドサイトの両方がある場合は、次の追加オプションを使用できます。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files):]** オンプレミスの APIC サイトとクラウド APIC サイトの両方に設定をプッシュし、オンプレミスとクラウドサイト間のエンドツーエンドインターコネクトを有効にします。

さらに、このオプションでは、IPN デバイスから Cisco クラウドサービスルータ (CSR) への接続できるようにするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files):]** 両方のクラウド APIC サイトに設定をプッシュし、クラウドサイトと外部デバイス間のエンドツーエンドインターコネクトを有効にします。

さらに、このオプションでは、外部デバイスから、自分のクラウドサイトに展開された Cisco クラウドサービスルータ (CSR) へ接続できるようにするための、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** 構成情報を含む zip ファイルをダウンロードします。これは、IPN デバイスから Cisco Cloud Services Router (CSR) への接続を、構成を展開することなく可能にするために用いるものです。

- **[外部デバイス設定ファイルのみをダウンロード (Download External Device config files only):]** 構成情報を含む zip ファイルをダウンロードします。これは、外部デバイスから Cisco Cloud Services Router (CSR) への接続を、構成を展開することなく可能にするために用いるものです。

ステップ 2 確認ウィンドウで **[はい (Yes)]** をクリックします。

[展開が開始されました。個々のサイトの展開ステータスメッセージについては、左側のメニューを参照してください (Deployment started, refer to left menu for individual site deployment status)] というメッセージにより、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで、各サイトの進行状況を確認できます。

次のタスク

インフラオーバーレイとアンダーレイの構成設定が、すべてのサイトのコントローラとクラウド CSR に展開されます。残った最後の手順では、[サイト接続性情報の更新 \(161 ページ\)](#) で説明するように、IPN デバイスをクラウド CSR のトンネルを使用して設定します。

オンプレミスとクラウドサイト間の接続の有効化

オンプレミス サイトまたはクラウドサイトのみがある場合は、このセクションをスキップできます。

ここでは、オンプレミス APIC サイトとクラウド APIC サイト間の接続を有効にする方法について説明します。

デフォルトでは、Cisco Cloud APIC は冗長 Cisco Cloud サービス ルータ 1000V のペアを展開します。この項の手順では、2つのトンネルを作成します。1つはオンプレミスの IPsec デバイスからこれらの各 Cisco Cloud サービス ルータ 1000V に対する IPsec トンネルです。複数のオンプレミス IPsec デバイスがある場合は、各オンプレミスデバイスの CSR に同じトンネルを設定する必要があります。

次の情報は、オンプレミスの IPsec ターミネーションデバイスとして Cisco Cloud サービス ルータ 1000V のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

ステップ 1 クラウドサイトに導入された CSR とオンプレミスの IPsec ターミネーションデバイスとの間の接続を有効にするために必要な必要な情報を収集します。

[インフラ設定の展開 \(173 ページ\)](#) の手順の一部として、Nexus Dashboard Orchestrator の **[IPN デバイス設定ファイルの展開とダウンロード (Deploy & Download IPN Device config files)]** オプションまたは **[IPN デバイス設定ファイルのダウンロード (IPN Device config files only)]** オプションを使用して、必要な設定の詳細を取得できます。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

最初の CSR の詳細は、Nexus Dashboard Orchestrator からダウンロードした ISN デバイスのコンフィギュレーションファイルで確認できますが、次のフィールドには、特定の展開の重要な値が示されます。

- `<first-csr-tunnel-id>` : このトンネルに割り当てる一意のトンネル ID です。
- `<first-csr-ip-address>` : 最初の CSR の 3 番目のネットワーク インターフェイスのパブリック IP アドレスです。

トンネルの宛先は、アンダーレイ接続のタイプによって異なります。

- アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
- アンダーレイがプライベート接続 (AWS の DX や Azure の ER など) を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。
- `<first-csr-preshared-key>` : 最初の CSR の事前共有キーです。
- `<onprem-device-interface>` : Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用されるインターフェイスです。
- `<onprem-device-ip-address>` : Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用される、`<interface>` インターフェイスの IP アドレスです。
- `<peer-tunnel-for-onprem-IPsec-to-first-CSR>` : 最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- `<process-id>` : OSPF プロセス ID です。
- `<area-id>` : OSPF エリア ID です。

次の例は、Nexus Dashboard Orchestrator リリース 3.3(1) および Cloud APIC リリース 5.2(1) 以降でサポートされている IKEv2 プロトコルを使用したサイト間接続設定を示しています。IKEv1 を使用している場合は、NDO からダウンロードした IPN 設定ファイルの外観が若干異なる場合がありますが、原則は同じです。

```
crypto ikev2 proposal ikev2-proposal-default
  encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
  integrity sha512 sha384 sha256 sha1
  group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
  proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
  peer peer-ikev2-keyring
    address <first-csr-ip-address>
    pre-shared-key <first-csr-preshared-key>
  exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
  match address local interface <onprem-device-interface>
  match identity remote address <first-csr-ip-address> 255.255.255.255
  identity local address <onprem-device-ip-address>
  authentication remote pre-share
```

```

    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-<first-csr-tunnel-id> esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    set transform-set infra:overlay-1-<first-csr-tunnel-id>
exit

interface tunnel 2001
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <onprem-device-interface>
    tunnel destination <first-csr-ip-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    ip mtu 1400
    ip tcp adjust-mss 1400
    ip ospf <process-id> area <area-id>
    no shut
exit

```

例 :

```

crypto ikev2 proposal ikev2-proposal-default
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001
    peer peer-ikev2-keyring
        address 52.12.232.0
        pre-shared-key 1449047253219022866513892194096727146110
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-2001
    ! Please change GigabitEthernet1 to the appropriate interface
    match address local interface GigabitEthernet1
    match identity remote address 52.12.232.0 255.255.255.255
    identity local address 128.107.72.62
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-2001
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-2001 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-2001

```



```

set pfs group14
set ikev2-profile ikev2-infra:overlay-1-2001
set transform-set infra:overlay-1-2001
exit

! These tunnel interfaces establish point-to-point connectivity between the on-prem device and the
cloud Routers
! The destination of the tunnel depends on the type of underlay connectivity:
! 1) The destination of the tunnel is the public IP of the cloud Router interface if the underlay
is via internet
! 2) The destination of the tunnel is the private IP of the cloud Router interface if the underlay
is via private
connectivity like DX on AWS or ER on Azure

interface tunnel 2001
ip address 5.5.1.26 255.255.255.252
ip virtual-reassembly
! Please change GigabitEthernet1 to the appropriate interface
tunnel source GigabitEthernet1
tunnel destination 52.12.232.0
tunnel mode ipsec ipv4
tunnel protection ipsec profile infra:overlay-1-2001
ip mtu 1400
ip tcp adjust-mss 1400
! Please update process ID according with your configuration
ip ospf 1 area 0.0.0.1
no shut
exit

```

ステップ4 2番目、および設定する必要があるその他のCSRについて、これらの手順を繰り返します。

ステップ5 オンプレミスのIPsecデバイスでトンネルがアップしていることを確認します。

現在のステータスを表示するには、次のコマンドを使用します。両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

```

ISN_CSR# show ip interface brief | include Tunnel
Interface          IP-Address      OK? Method Status          Protocol
Tunnel1000         30.29.1.2       YES manual up              up
Tunnel1001         30.29.1.4       YES manual up              up

```




第 17 章

CloudSec 暗号化

- [Cisco ACI CloudSec 暗号化 \(179 ページ\)](#)
- [要件と注意事項 \(180 ページ\)](#)
- [CloudSec 暗号化に関する用語 \(183 ページ\)](#)
- [CloudSec の暗号化と復号の処理 \(184 ページ\)](#)
- [CloudSec 暗号化キーの割り当てと配布 \(187 ページ\)](#)
- [CloudSec 暗号化のための Cisco APIC の設定 \(190 ページ\)](#)
- [Nexus Dashboard Orchestrator GUI を使用した CloudSec 暗号の有効化 \(193 ページ\)](#)
- [スイッチでの CloudSec 構成の確認 \(194 ページ\)](#)
- [スパインスイッチ メンテナンス中のキー再生成プロセス \(196 ページ\)](#)

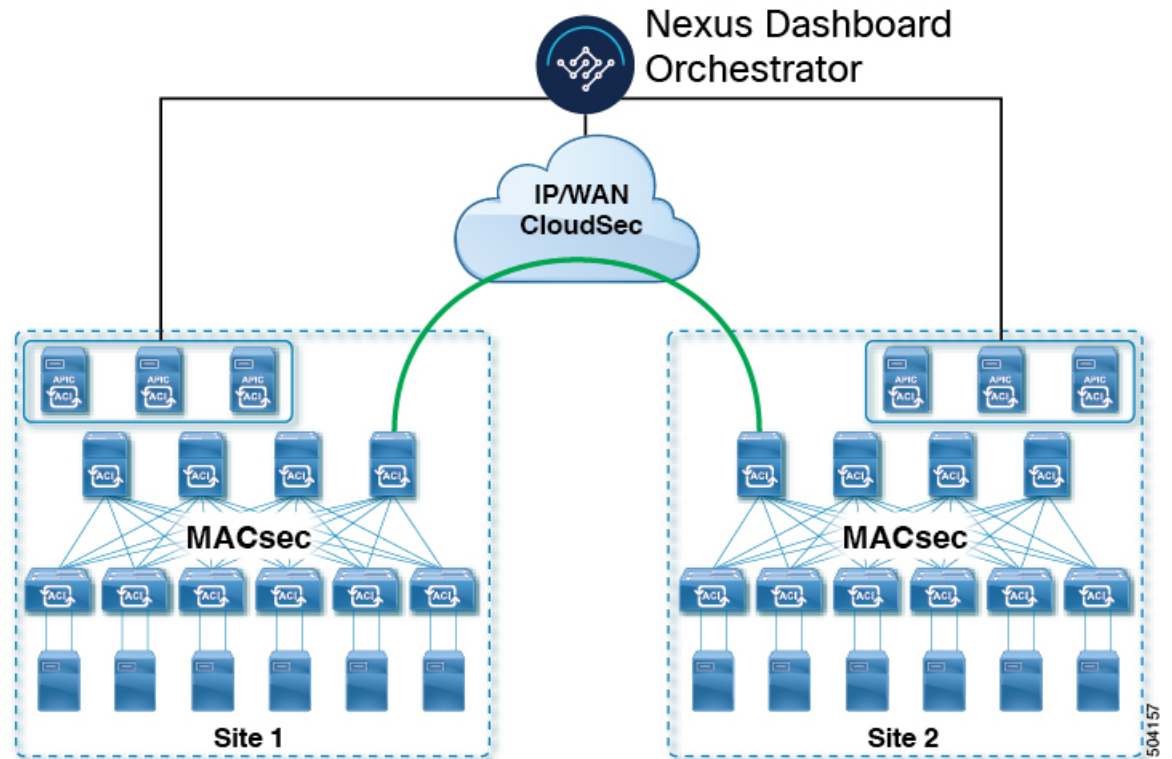
Cisco ACI CloudSec 暗号化

ほとんどの Cisco ACI 展開で、ディザスタリカバリとスケーリングに対処する Multi-Site アーキテクチャを採用しているため、ローカルサイト内で MACsec 暗号化を使用する現在のセキュリティ実装は、複数のサイトにわたるデータセキュリティと整合性を保証するには不十分になっています。それらのサイトは、安全でない外部 IP ネットワークによって接続されており、個別のファブリックを相互接続しているからです。Nexus Dashboard Orchestrator リリース 2.0(1) は、トラフィックのサイト間暗号化を提供するために設計された CloudSec 暗号化を導入しています。

Multi-Site トポロジはサイト間の接続を提供するために、3つのトンネルエンドポイント (TEP) IP アドレス (Overlay Multicast TEP、Overlay Unicast TEP、および External TEP Pool) を使用します。これらの TEP アドレスは、Nexus Dashboard Orchestrator の管理者により設定され、各サイトの Cisco APIC にプッシュダウンされ、その後スパインスイッチで設定されます。これらの3つのアドレスは、トラフィックがリモートサイトに送信されるタイミングを決定するために使用されます。この場合、2つのスパインスイッチ間に暗号化された CloudSec トンネルが作成され、サイト間ネットワーク (ISN) を介して2つのサイト間の物理接続が提供されます。

次の図は、ローカルサイトトラフィックの MACsec とサイト間トラフィックの暗号化に CloudSec を組み合わせた全体的な暗号化アプローチを示しています。

図 16: CloudSec 暗号化



要件と注意事項

CloudSec 暗号化を設定する場合は、次の注意事項が適用されます。

- CloudSec は、Nexus 9000 サイト間ネットワーク (ISN) インフラストラクチャを使用して検証されています。ISN インフラストラクチャがさまざまなデバイスで構成されている場合、またはデバイスが不明な場合 (サービスプロバイダーから購入した回線の場合など)、ASR1K ルーターは、ACI スパイン (各サイトに展開された ASR1K デバイスの個別のペアを使用)、または Nexus 9000 ISN ネットワークに直接接続するファースト ホップ デバイスである必要があります。パディングフィックスアップが有効になっている ASR1K ルーターにより、CloudSec トラフィックはサイト間の任意の IP ネットワークを通過できます。

ASR1K ルータを構成するには:

1. デバイスにログインします。
2. UDP ポートを構成します。



- (注) リリース 3.7(1) 以降を実行していて、IANA が割り当てたポート 8017 を使用するように CloudSec を構成する場合は、代わりに次のコマンドでそのポートを指定します。

```
ASR1K(config)# platform cloudsec padding-fixup dst-udp-port 9999
```

3. 設定を確認します。

次の出力で、前の手順で構成したポート (8017 または 9999) が表示されていることを確認します。

```
ASR1K# show platform software ip rp active cloudsec
CloudSec Debug: disabled
CloudSec UDP destination port: enabled
1st UDP destination port: 9999
2nd UDP destination port: 0
3rd UDP destination port: 0
```

```
ASR1K# show platform software ip fp active cloudsec
CloudSec Debug: disabled
CloudSec UDP destination port: enabled
1st UDP destination port: 9999
2nd UDP destination port: 0
3rd UDP destination port: 0
```

- CloudSec 暗号化を無効にしようとしたときに1つ以上のスパインスイッチがダウンした場合、スイッチがアップするまで、これらのスイッチでディセーブルプロセスは完了しません。これにより、スイッチが再起動したときにパケットがドロップされることがあります。

CloudSec 暗号化を有効または無効にする前に、ファブリック内のすべてのスパインスイッチが稼働していること、または完全に停止していることを確認することを推奨します。

- Nexus Dashboard Orchestrator リリース 3.7(1) 以降では、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成できます。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。Orchestrator リリース 3.7(1) 以降は、サイト間の CloudSec 暗号化に IANA が予約した公式ポート 8017 を使用するように構成できます。



- (注) IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに1つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート (IANA Reserve UDP Port)]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

- CloudSec 暗号化機能は、次の機能ではサポートされません。
 - 高精度時間プロトコル (PTP)
 - リモート リーフ ダイレクト
 - 仮想ポッド (vPod)
 - SDA
 - リモート リーフまたはマルチポッド構成
 - サイト間 L3Out (サイトが 5.2(4) より前の Cisco APIC リリースを実行している場合)。
CloudSec は、リリース 5.2(4) 以降を実行している APIC サイトのサイト間 L3Out でサポートされています。

要件

CloudSec 暗号化機能では、次のものがが必要です。

- Cisco ACI スパイン/リーフアーキテクチャと 1 台の Cisco APIC クラスタ (各サイト用)
- 各サイトを管理する Cisco Nexus Dashboard Orchestrator
- ファブリックのデバイス (リーフのみ) ごとに 1 つの **Advantage** または **Premier** ライセンス
- デバイスが固定スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XF** アドオン ライセンス
- デバイスがモジュール スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XM** アドオン ライセンス

次の表に、CloudSec 暗号化に対応したハードウェア プラットフォームとポート範囲を示します。

ハードウェア プラットフォーム	ポート範囲
N9K C9364C スパインスイッチ	ポート 49-64
N9K-C9332C スパインスイッチ	ポート 25-32
N9K-X9736C-FX ラインカード	ポート 29-36

CloudSec がサイトに対して有効になっているが、暗号化がポートでサポートされていない場合、サポートされていないインターフェイスのエラーメッセージで障害が発生します。

CloudSec 暗号化の packets encapsulation は、DWDM-C SFP10G などの Cisco QSFP から SFP へのアダプタ (QSA) がサポートされている光ファイバで使用されている場合にサポートされます。サポートされている光ファイバの完全なリストは、<https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html> のリンクから入手できます。

IANA が割り当てたポートと Orchestrator のダウングレードの使用

次のセクションで説明されているように、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成した場合、Orchestrator サービスをリリース 3.7(1) より前のリリースにダウングレードする場合、いくつかの手順を実行する必要があります。

Nexus Dashboard Orchestrator を IANA ポートがサポートされていないリリースにダウングレードする前に:

1. すべての管理対象サイトの CloudSec 暗号化を無効にします。
2. インフラ構成設定で **IANA 予約済み UDP ポート オプション** を無効にします。
3. 以前に有効にしたすべてのサイトで CloudSec 暗号化を再度有効にします。
4. 通常どおり、Orchestrator サービスをダウングレードします。

CloudSec 暗号化に関する用語

CloudSec 暗号化機能は、サイト間の初期キーとキー再生成の要件に対して、安全なアップストリーム対称キーの割り当てと配布方法を提供します。この章では、次の用語を使用します。

- アップストリーム デバイス - CloudSec 暗号化ヘッダーを追加し、ローカルで生成された対称暗号化キーを使用してリモート サイトへの送信時に VXLAN パケット ペイロードの暗号化を行うデバイス。
- ダウンストリーム デバイス - CloudSec 暗号化ヘッダーを解釈し、リモート サイトで生成された暗号化キーを使用して受信時に VXLAN パケットペイロードの復号化を行うデバイス。
- アップストリーム サイト - 暗号化された VXLAN パケットを発信するデータ センター ファブリック。
- ダウンストリーム サイト - 暗号化されたパケットを受信して復号するデータ センター ファブリック。
- TX キー - クリアな VXLAN パケット ペイロードを暗号化するために使用される暗号化キー。ACI では、1 つの TX キーがすべてのリモート サイトに対してアクティブであることができます。
- RX キー - 暗号化された VXLAN パケット ペイロードを復号するために使用される暗号化キー。ACI では、2 つの RX キーをリモート サイトごとにアクティブにできます。2 つの RX キーをキーの再生成プロセス中に同時にアクティブにすることができます。ダウストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。
- 対象キー - 同じ暗号化キーを使用して、アップストリーム デバイスとダウンストリーム デバイスによるパケットストリームの暗号化 (TX キー) と復号 (RX キー) をそれぞれ行う場合。

- キーの再生成 – 古いキーの有効期限が切れた後、すべてのダウンストリーム サイトの古いキーを新しいキーに置き換えるためにアップストリームサイトによって開始されたプロセス。
- 安全なチャネル識別子 (SCI) – サイト間のセキュリティ関連付けを表す 64 ビット識別子。CloudSec ヘッダーの暗号化されたパケットで送信され、パケットの復号化のためにダウンストリームデバイスの RX キーを取得するために使用されます。
- アソシエーション番号値 (AN) – 暗号化されたパケットのCloudSecヘッダーで送信される2ビットの数値(0, 1, 2, 3)。これは、復号化のために SCI とともにダウンストリームデバイスでキーを導出するために使用されます。これにより、ダウンストリームデバイスで複数のキーをアクティブにして、キーの再生成操作の後で、同じアップストリームデバイスからの異なるキーを使用したパケットの順序どおりでない到着を処理できます。

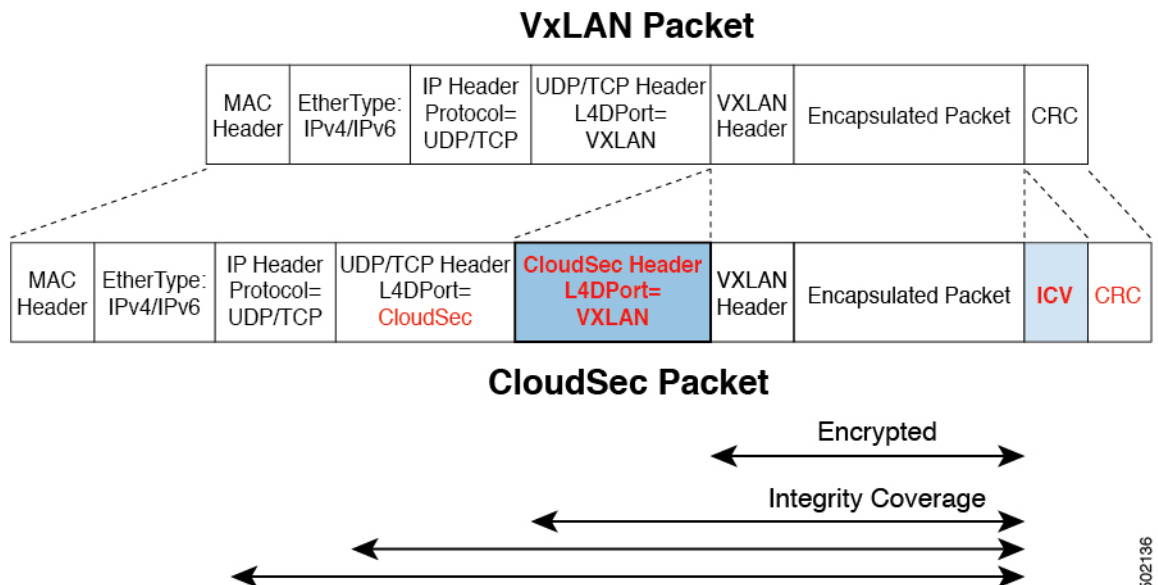
ACI では、2つのアクティブな RX キーには2つのアソシエーション番号値 (0 または 1) のみを使用され、TX キーには常に1つのアソシエーション番号値 (0 または 1) のみを使用されます。
- 事前共有キー (PSK) – CloudSec TX および RX キーを生成するためのランダム シードとして使用するには、Cisco APIC GUI で1つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64文字の長さの16進数ストリングでなければなりません。Cisco APIC は最大256の事前共有キーをサポートします。

CloudSec の暗号化と復号の処理

リリース2.0(1)以降では、データセキュリティと整合性の両方に対応する、完全に統合されたシンプルでコスト効率の高いソリューションを提供するために、Multi-Site は Multi-Site ファブリック間の送信元から宛先への完全なパケット暗号化を可能にする CloudSec 暗号化機能を提供します。

次の図は、CloudSec カプセル化の前後のパケット ダイアグラムと、その後の暗号化および復号化プロセスの説明を示しています。

図 17: CloudSec パケット



502136

パケット暗号化

次に、CloudSec が発信トラフィック パケットを処理する方法の概要を示します。

- パケットは、外部 IP ヘッダ宛先アドレス フィールドとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、フィルタされたパケットは暗号化の対象としてマークされます。
- 暗号化に使用するオフセットは、パケットのフィールドに基づいて計算されます。たとえば、オフセットは、802.1q VLAN があるかどうか、またはパケットが IPv4 または IPv6 パケットであるかどうかによって異なります。
オフセットは自動的に決定され、ユーザーには表示されません。
- 暗号キーはハードウェアテーブルでプログラムされ、パケット IP ヘッダーを使用してテーブルから検索されます。

パケットに暗号化のマークが付けられると、暗号キーがロードされ、暗号化を開始するパケットの先頭からのオフセットが判明すると、次の追加の手順が実行されます。

- UDP 宛先ポート番号は、UDP ヘッダーから CloudSec フィールドにコピーされ、パケットが暗号解読されるときにリカバリされます。
- UDP 宛先ポート番号は、CloudSec パケットであることを示すために上書きされます。

3.7(1) より前のリリースでは、ポートは Cisco 独自のレイヤ 4 ポート番号 9999 で上書きされます。

IANA が割り当てたポート 8017 を使用するように CloudSec を構成できるリリース 3.7(1) 以降では、使用される宛先ポート番号は、このオプションを有効にしているかどうかに応じて 9999 または 8017 のいずれかです。

- [UDP長(UDP length)] フィールドは、追加されるバイト数を反映するように更新されます。
- CloudSec ヘッダーは、UDP ヘッダーの後に直接挿入されます。
- 整合性チェック値 (ICV) は、ペイロードと CRC の間のパケットの最後に挿入されます。
- ICV では、128 ビットの初期化ベクトルを構築する必要があります。CloudSec の場合、ICV のために送信元 MAC アドレスを使用すると、SCI ごとのプログラム可能な値に置き換えられます。
- CRC は、パケットのコンテンツの変更を反映するように更新されます。

パケットの暗号解読

CloudSec が受信パケットを処理する方法は、上記で説明した発信パケット アルゴリズムと対称的です。

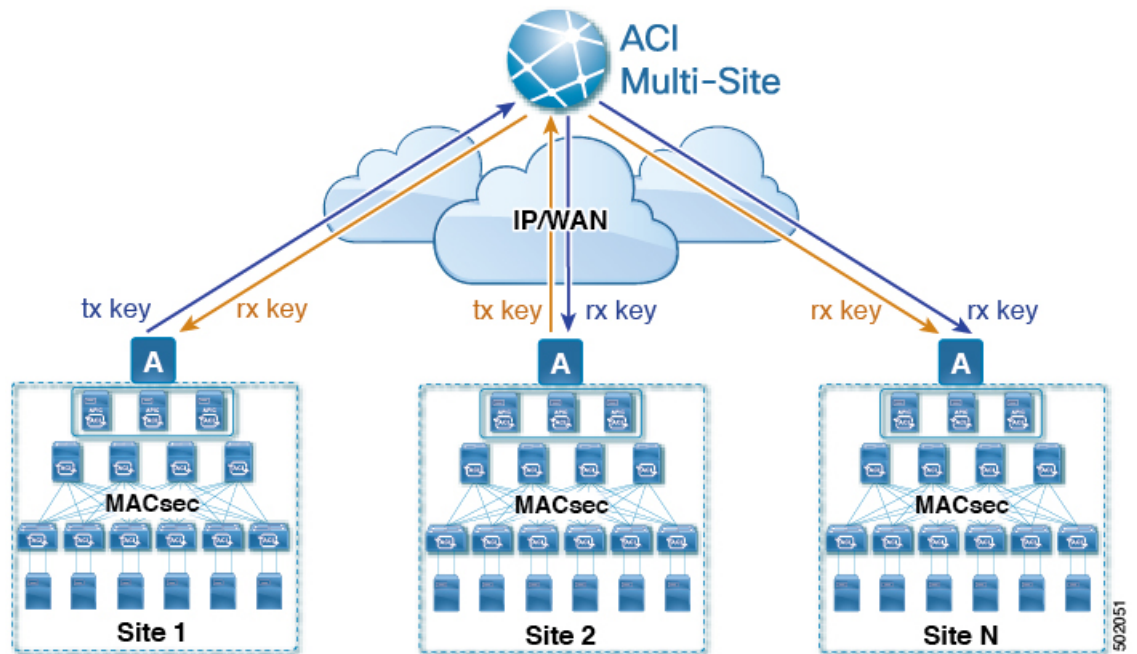
- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

ICV 検証に合格すると、追加フィールドが削除され、UDP 宛先ポート番号が CloudSec ヘッダーから UDP ヘッダーに移動され、CRC が更新され、パケットの暗号解読と CloudSec ヘッダーの削除後に宛先に転送されます。そうでない場合、パケットはドロップされます。
- 復号化キーは、受信した CloudSec パケットの外部 IP ヘッダーのソースアドレスフィールド、CloudSec ヘッダーの SCI、および AN 番号フィールドを使用してキーストアから取得されます。
- パケットが CloudSec パケットでない場合、パケットはそのまま残ります。

CloudSec 暗号化キーの割り当てと配布

初期キー構成

図 18: CloudSec キーの配布



次に、上記の図に示されている CloudSec 暗号化キーの初期割り当ておよび配信プロセスの概要を示します。

- アップストリームサイトの Cisco APIC は、サイトから送信された VXLAN パケットのデータ暗号化に使用されるためのローカル対称キーを生成します。アップストリームサイトが暗号化に使用すると同じキーが、ダウンストリームリモート受信サイトのパケットの復号に使用されます。

各サイトはほかのサイトに送信するトラフィックのためのアップストリームサイトです。複数のサイトが存在する場合、各サイトは独自のサイトツーサイトキーを生成し、そのキーを暗号化に使用してからリモートサイトに送信します。

- 生成された対称キーは、ダウンストリーム リモート サイトに配布するために、アップストリーム サイトの Cisco APIC によって Nexus Dashboard Orchestrator (NDO) にプッシュされます。
- NDO はメッセージブローカとして機能し、生成された対称キーをアップストリーム サイトの Cisco APIC から収集し、それをダウンストリーム リモート サイトの Cisco APIC に配布します。

キーは、キー暗号化キー (KEK) を使用して暗号化され、TLS ベースのチャンネルを介して配布されます。

- 各ダウンストリームサイトの Cisco APIC は、受信したキーを、キーを生成したアップストリームサイトからのトラフィックを受信することを目的としたローカルスパインスイッチの RX キーとして設定します。
- 各ダウンストリームサイトの Cisco APIC は、ローカル スパイン スイッチから RX キーの展開ステータスを収集し、NDO にプッシュします。
- NDO は、すべてのダウンストリームリモートサイトからアップストリームサイトの Cisco APIC に戻って、主要な展開ステータスを中継します。
- アップストリームサイトは Cisco APIC、すべてのダウンストリーム リモート サイトから受信したキー展開ステータスが成功したかどうかを確認します。
 - ダウンストリームデバイスから受信した展開ステータスが成功した場合、アップストリームサイトはスパインスイッチの TX キーとしてローカル対称キーを展開し、ダウンストリームサイトに送信される VXLAN パケットの暗号化を有効にします。
 - ダウンストリームデバイスから受け取った展開ステータスが失敗した場合、失敗した Cisco APIC サイトで障害が発生し、NDO で構成された「セキュアモード」設定に基づいて処理されます。「セキュアが必須 (must secure)」モードでは、パケットはドロップされ、「セキュアであるべき (should secure)」モードでは、パケットは宛先サイトに平文 (暗号化されていない) で送信されます。



(注) 現在のリリースでは、モードは常に「セキュアであるべき (should secure)」に設定されており、変更できません。

キー再生成プロセス

生成された各 TX/RX キーは、設定された時間が経過すると有効期限が切れます。デフォルトでは、キーの有効期限は 15 分に設定されています。TX/RX キーの初期セットが期限切れになると、キー再生成プロセスが行われます。

キーの再割り当てプロセスには、同じ一般的なキーの割り当てと配布フローが適用されます。キー再生成プロセスは「ブレイク前に作成 (make before break)」ルールに従います。つまり、新しい TX キーがアップストリームサイトに展開される前に、ダウンストリームサイトのすべての RX キーが展開されます。これを実現するために、アップストリームサイトは、ローカルアップストリームサイトのデバイスに新しい TX キーを構成する前に、ダウンストリームサイトからの新しい RX キーの展開ステータスを待ちます。

ダウンストリームサイトが新しい RX キーの展開で障害ステータスを報告した場合、キー再生成プロセスは終了し、古いキーはアクティブなままになります。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。



- (注) スパインスイッチのメンテナンス中のキー再生成プロセスに関しては、特別な注意が必要です。詳細については、[スパインスイッチメンテナンス中のキー再生成プロセス \(196ページ\)](#)を参照してください。

キー再生成プロセスの失敗

ダウンストリームサイトがキー再生成プロセスによって生成された新しい暗号化キーの展開に失敗した場合、新しいキーは破棄され、アップストリーム デバイスは以前の有効なキーを TX キーとして引き続き使用します。このアプローチにより、アップストリームサイトは、ダウンストリームサイトのセットごとに複数の TX キーを維持する必要がなくなります。ただし、このアプローチでは、いずれかのダウンストリームサイトでキー再生成の展開エラーが発生し続ける場合、キー更新プロセスが遅延する可能性もあります。マルチサイト管理者は、キー再生成を成功させるために、キーの展開の失敗の問題を修正するための行動を取ることが期待されています。

Cisco APICキー管理のロール

Cisco APIC は、キー割り当て (初期キーとキー再配布の両方)、スパインスイッチからのキー展開ステータスメッセージの収集、および他のサイトへの配布のための各キーのステータスに関する Nexus Dashboard Orchestrator への通知に責任をもちます。

キー管理における Nexus Dashboard Orchestrator の役割

Nexus Dashboard Orchestrator は、アップストリームサイトから TX キー (初期キーと後続のキーの再生成の両方) を収集し、RX キーとして展開するためにすべてのダウンストリームサイトに配布します。NDO はまた、ダウンストリームサイトから RX キーの展開ステータス情報を収集し、成功した RX キー展開ステータスで TX キーを更新するために、アップストリームサイトに通知します。

アップストリーム モデル

MPLS など、ダウンストリーム キー割り当てを使用する他のテクノロジーとは対照的に、CloudSec のアップストリーム モデルには次の利点があります。

- このモデルはシンプルで、運用とネットワークへの導入が容易です。
- モデルは、マルチサイトのユースケースに適しています。
- 複数の宛先サイトに送信される複製パケットの各コピーに同じキーと CloudSec ヘッダーを使用できるため、マルチキャストトラフィックに利点があります。ダウンストリームモデルでは、各コピーは暗号化中にサイトごとに異なるセキュリティキーを使用する必要があります。
- 障害が発生した場合のトラブルシューティングが容易になり、複製されたユニキャストパケットとマルチキャストパケットの両方に対して、送信元から宛先へのパケットのトレーサビリティが一貫して向上します。

CloudSec 暗号化のための Cisco APIC の設定

CloudSec 暗号と復号キーを生成するために、Cisco APIC で使用する 1 個以上の事前共有キー (PSK) を構成する必要があります。PSK は再キー プロセス中のランダム シードとして使用されます。複数の PSK が設定される場合、各再キー プロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。

暗号キーの生成に対するシードとして PSK が使用されるため、複数の PSK の設定では生成された暗号キーの長時間にわたる脆弱性を下げることにより、追加のセキュリティを提供します。



(注) Cisco APIC で事前共有キーが構成されていない場合、CloudSec はそのサイトに対して有効にはなりません。その場合、マルチサイトで CloudSec 設定をオンにすると、障害が生じます。

いつでも新しい PSK で前に追加した PSK を更新したい場合、新しいキーを追加するときと同様の手順を繰り返すだけです。インデックスは既存のものを指定してください。

1 つ以上の事前共有キーを次の 3 通りの方法のいずれかを使用して設定できます。

- [GUI を使用した CloudSec 暗号化の Cisco APIC の設定 \(190 ページ\)](#) で説明されている Cisco APIC GUI の使用
- [NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定 \(191 ページ\)](#) で説明されている Cisco APIC NX-OS スタイルの CLI の使用
- [REST API を使用した CloudSec 暗号化の Cisco APIC の設定 \(192 ページ\)](#) で説明されている Cisco APIC REST API の使用

GUI を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC GUI を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

ステップ 1 APIC にログインします。

ステップ 2 [テナント]> [インフラ]> [ポリシー]> [CloudSec 暗号化]に移動します。

ステップ 3 SA キーの有効期限を指定します。

このオプションは、各キーが有効な時間(分)を指定します。それぞれの生成された TX/RX キーは、再キー プロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5~1440 分の範囲で入力できます。

ステップ 4 [事前共有キー]テーブルの + アイコンをクリックします。

ステップ 5 追加する事前共有キーのインデックスを指定し、その後、事前共有キー自体を指定します。

[インデックス (Index)] フィールドは、事前共有キーを使用する順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスは 1 ~ 256 でなければなりません。各事前共有キーは、64 文字の 16 進数文字列である必要があります。

NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定

このセクションでは、Cisco APIC NX OS Style CLI を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーション モードを入力します。

例 :

```
apicl# configure
apicl (config)#
```

ステップ 3 デフォルト CloudSec プロファイルのコンフィギュレーション モードを入力します。

例 :

```
apicl (config)# template cloudsec default
apicl (config-cloudsec)#
```

ステップ 4 事前共有キー (PSK) の有効期限を指定します。

このオプションは、各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キー プロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5 ~ 1440 分の範囲で入力できます。

例 :

```
apicl (config-cloudsec)# sakexpirytime <duration>
```

ステップ 5 1 つまたは複数の事前共有キーを指定します。

次のコマンドでは、設定している PSK のインデックスと PSK 文字列自体を指定します。

例 :

```
apicl (config-cloudsec)# pskindex <psk-index>
apicl (config-cloudsec)# pskstring <psk-string>
```

<psk-index> パラメータは、事前共有キーが使用される順序を指定します。最後 (最上位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスは 1 ~ 256 でなければなりません。

<psk-string> パラメータは、実際の PSK を指定します。これは、64 文字の 16 進数文字列である必要があります。

ステップ 6 (オプション) 現在の PSK 設定を表示します。

現在設定されている PSK の数とその期間を表示するには、次のコマンドを使用します。

例：

```
apic1(config-cloudsec)# show cloudsec summary
```

REST API を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC REST API を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

PSK 有効期限、インデックス、文字列を設定します。

次の XML POST で、次を置換します。

- 各 PSK の期限をもつ **sakExpiryTime** の値。

この **sakExpiryTime** パラメータは各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キー プロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5 ~1440 分の範囲で入力できます。

- 設定している PSK のインデックスをもつ **インデックス** の値。

インデックス パラメータは、事前共有キーが使用される順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスは 1 ~ 256 でなければなりません。

- 設定している PSK のインデックスをもつ **pskString** の値。

pskString パラメータは実際の PSK を指定します。これは 16 進文字列で長さ 64 文字でなければなりません。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">
  <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey="false" status=""
  >
    <cloudsecPreSharedKey index="1"
    pskString="12345678123456781234567812345678123456781234567812345678123456781234567812345678" status=""/>
  </cloudsecIfPol>
</fvTenant>
```


Nexus Dashboard Orchestrator GUI を使用した CloudSec 暗号の有効化

CloudSec 暗号化は、サイトごとに個別に有効または無効にすることができます。ただし、2つのサイト間の通信は、この機能が両方のサイトで有効になっている場合にのみ暗号化されません。

始める前に

2つ以上のサイト間で CloudSec 暗号化を有効にする前に、次のタスクを完了しておく必要があります。

- 『Cisco APIC のインストール、アップグレード、ダウングレードガイド』で説明されているように、複数のサイトに Cisco APIC クラスタをインストールして設定します。
- 『Cisco Nexus Dashboard Orchestrator インストールおよびアップグレードガイド』の説明に従って、Nexus Dashboard Orchestrator をインストールし、設定します。
- 『Cisco ACI マルチサイト コンフィギュレーションガイド』の説明に従って、各 Cisco APIC サイトを Nexus Dashboard Orchestrator に追加します。

ステップ 1 Nexus Dashboard Orchestrator にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メインウィンドウの右上にある [構成 (Configure)] ボタンをクリックします。

ステップ 4 (オプション) [一般設定 (General Settings)] ページの [コントロールプレーンの構成 (Control Plane Configuration)] タブで、[IANA 予約済み UDP ポート (IANA Reserved UDP Port)] オプションを有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

(注) IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに1つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、[IANA 予約 UDP ポート (IANA Reserve UDP Port)] オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

ステップ 5 左側のサイドバーから、CloudSec 設定を変更するサイトを選択します。

ステップ 6 右側のサイドバーで、[Cloudsec 暗号化 (Cloudsec encryption)] 設定を切り替えて、サイトの CloudSec 暗号化機能を有効または無効にします。

スイッチでの CloudSec 構成の確認

次のコマンドを使用すると、Nexus Dashboard Orchestrator から CloudSec 暗号化を有効にした後、スパインスイッチに展開された現在の CloudSec 構成を確認できます。

ステップ1 スパインスイッチにログインします。

ステップ2 `show cloudsec sa interface all` コマンドを実行して、CloudSec 構成を表示します。

次の出力で、各インターフェイスについて次のことを確認します。

- Operational Status の値は UP を示します。
- Control 値は、CloudSec 暗号化に現在使用されている UDP ポートを示すため、すべての CloudSec 対応サイトのすべてのインターフェイスで同じです。

次の例は、デフォルトのシスコ独自の UDP ポート (`deprecatedUdpPort`) を示しています。IANA が割り当てたポート 8017 を使用するように CloudSec を構成すると、**[制御]** フィールドには代わりに `ianaUdpPort` が表示されます。

```
spine1# show cloudsec sa interface all
=====
Interface: Eth1/49.49(0x1a030031) Physical Interface: Eth1/49(0x1a030000)
Operational Status: UP Retry: Off Control: deprecatedUdpPort
-----
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
Pod-Id: 1
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 0 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.520-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
-----
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 2 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.563-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 1 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 3 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.442-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 0 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
Hardware Index: 2 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.453-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
-----
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
```

```
Hardware Index: 1 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.549-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 1 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 1 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:36.501-08:00 Retry: Off
Uptime: 11 hours 30 mins 46 secs
RX Key: ***** Assoc Num: 0 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
Hardware Index: 0 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.495-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs

=====
Interface: Eth1/50.50(0x1a031032) Physical Interface: Eth1/50(0x1a031000)
Operational Status: UP Retry: Off Control: deprecatedUdpPort
-----
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
Pod-Id: 1
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 1 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.577-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
-----
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 0 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.537-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 1 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 1 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:36.463-08:00 Retry: Off
Uptime: 11 hours 30 mins 46 secs
RX Key: ***** Assoc Num: 0 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
Hardware Index: 0 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.416-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs

-----
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
-----
TX Key: ***** Assoc Num: 1 Sci: 0x10002
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 2 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.593-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 0 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
Hardware Index: 2 Operational Status: UP Control: NONE
Last Updated: PST 2022-01-11 23:26:37.481-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
RX Key: ***** Assoc Num: 1 Sci: 0x20001
Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
Hardware Index: 3 Operational Status: UP Control: NONE
```

Last Updated: PST 2022-01-11 23:26:37.507-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs

スパインスイッチメンテナンス中のキー再生成プロセス

次に、この機能が有効になっているスパインスイッチの一般的なメンテナンスシナリオでの CloudSec キー再生成プロセスの概要を示します。

- **通常の解放:** CloudSec 対応スパインスイッチがデコミッションされると、CloudSec キー再生成プロセスが自動的に停止します。解放されたノードが再起動されるか、解放されたノードIDが次から削除されるまで、キー再生成プロセスは再度開始されません: Cisco APIC
- **スパインスイッチのソフトウェアアップグレード:** スパインスイッチがソフトウェアのアップグレードによりリロードされると、CloudSec キー再生成プロセスは自動的に停止します。キー再生成プロセスは、スパインスイッチのリロードが完了すると、再開されません。
- **メンテナンス (GIR モード):** CloudSec キー再生成プロセスは、[NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする \(196 ページ\)](#) に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、ノードがトラフィックを転送する準備が再度整った後にのみ、有効にできます。
- **Cisco APICからの解放と削除:** CloudSec キー再生成プロセスは、[NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする \(196 ページ\)](#) に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、Cisco APIC からノードが削除された後にのみ有効にできます。

NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、デコミッションとメンテナンスの切り替えなどです。このセクションは、Cisco APIC NX-OS Style CLI を使用して設定を切り替える方法を説明します。

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーションモードを入力します。

例:

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

ステップ 3 デフォルト CloudSec プロファイルのコンフィギュレーションモードを入力します。

例：

```
apicl(config)# template cloudsec default  
apicl(config-cloudsec)#
```

ステップ 4 キーの再生成プロセスを停止するか、再開します。

キーの再生成を停止するには：

例：

```
apicl(config-cloudsec)# stoprekey yes
```

キーの再生成プロセスを再開するには：

例：

```
apicl(config-cloudsec)# stoprekey no
```

REST API を使用したキー再生成プロセスの無効化と再有効化

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、でコミッションとメンテナンスの切り替えなどです。このセクションでは、Cisco APICREST API を使用して設定を切り替える方法について説明します。

ステップ 1 キー再生成プロセスは、次のXML メッセージを使用して無効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">  
  <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "true" status=""  
  />  
</fvTenant>
```

ステップ 2 キー再生成プロセスは、次のXML メッセージを使用して有効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">  
  <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""  
  />  
</fvTenant>
```



第 **IV** 部

機能と使用例

- [DHCPリレー](#) (201 ページ)
- [EPG 優先グループ](#) (211 ページ)
- [サイト内 L3Out](#) (215 ページ)
- [PBR を使用したサイト間 L3Out](#) (237 ページ)
- [レイヤ 3 マルチキャスト](#) (265 ページ)
- [IPN 全体での QoS の保持](#) (279 ページ)
- [SD-Access と ACI 統合](#) (285 ページ)
- [SD-WAN の統合](#) (307 ページ)
- [SR-MPLS 経由で接続されたサイト](#) (315 ページ)
- [vzAny コントラクト](#) (337 ページ)



第 18 章

DHCP リレー

- DHCP リレー ポリシー (201 ページ)
- 注意事項と制約事項 (202 ページ)
- DHCP リレー ポリシーの作成 (203 ページ)
- DHCP オプション ポリシーの作成 (204 ページ)
- DHCP ポリシーの割り当て (205 ページ)
- DHCP リレー コントラクトの作成 (206 ページ)
- APIC での DHCP リレー ポリシーの確認 (208 ページ)
- 既存の DHCP ポリシーの編集または削除 (208 ページ)

DHCP リレー ポリシー

通常、DHCP サーバが EPG の下に配置されている場合、その EPG 内のすべてのエンドポイントがアクセス権を持ち、DHCP を介して IP アドレスを取得できます。ただし、多くの導入シナリオでは、DHCP サーバが必要なすべてのクライアントと同じ EPG、BD、または VRF に存在していない可能性があります。このような場合、1つの EPG 内のエンドポイントが別のサイトに配置された別の EPG/BD にあるサーバから、またはファブリックに外部に接続され、L3Out 接続を介して到達可能なサーバから IP アドレスを取得できるように、DHCP リレーを設定できます。

Orchestrator GUI で DHCP リレー ポリシーを作成してリレーを設定できます。また、DHCP オプション ポリシーを作成して、特定の設定の詳細を提供するためにリレーポリシーで使用できる追加オプションを設定することもできます。使用可能なすべての DHCP オプションについては、[RFC 2132](#) を参照してください。

DHCP リレーポリシーを作成する場合は、DHCP サーバが存在する EPG (たとえば、`epg1`) または外部 EPG (たとえば、`ext epg1`) を指定します。DHCP ポリシーを作成した後、それをブリッジドメインに関連付けます。これにより、その EPG 内のエンドポイントが DHCP サーバに到達できるようになります。これにより、別の EPG (たとえば、`epg2`) に関連付けられます。最後に、リレー EPG (`epg1` または `epg1`) とアプリケーション EPG (`epg2`) 間の契約を作成し、通信を可能にします。作成した DHCP ポリシーは、ポリシーが関連付けられているブリッジドメインがサイトに展開されるときに、APIC にプッシュされます。

注意事項と制約事項

DHCP リレーポリシーは、次の警告でサポートされます。

- DHCP リレーポリシーは、Cisco APIC リリース 4.2(1) 以降を実行しているファブリックでサポートされています。
- DHCP サーバは、DHCP リレー エージェント情報オプション (オプション 82) をサポートしている必要があります。

ACI ファブリックが DHCP リレーとして動作する場合、DHCP リレーエージェント情報オプションは、クライアントの代わりにプロキシする DHCP 要求に挿入されます。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。

- DHCP リレーポリシーは、ユーザテナントまたは共通テナントでのみサポートされます。DHCP ポリシーは、インフラまたは管理テナントではサポートされていません。

ACI ファブリックで共有リソースとサービスを設定する場合は、共通テナントでこれらのリソースを作成することをお勧めします。これは、どのユーザテナントでも使用できます。

- DHCP リレーサーバは、DHCP クライアントまたは共通テナントと同じユーザテナントに存在する必要があります。

サーバとクライアントは、異なるユーザテナントに配置することはできません。

- DHCP リレーポリシーは、プライマリ SVI インターフェイスにのみ設定できます。

リレーポリシーを割り当てるブリッジドメインに複数のサブネットが含まれている場合、追加した最初のサブネットは SVI インターフェイスのプライマリ IP アドレスになります。追加のサブネットはセカンダリ IP アドレスとして設定されます。複数のサブネットを持つブリッジドメインを使用した設定のインポートなどの特定のシナリオでは、SVI のプライマリアドレスがセカンダリアドレスの1つに変更されることがあり、そのブリッジドメインの DHCP リレーが中断されることがあります。

Show ip interface vrf all コマンドを使用して、SVI インターフェイスの IP アドレスの割り当てを確認できます。

- ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジドメインを1つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジドメインを再展開する必要があります。
- L3Out 経由で到達可能な DHCP サーバとの VRF 間 DHCP リレーの場合、DHCP リレーパケットは、DHCP サーバに到達するためにサイトローカル L3Out を使用する必要があります。異なるサイト (サイト間 L3Out) の L3Out を使用するパケットはサポートされていません。
- 次の DHCP リレー設定はサポートされていません。
 - L3Out の背後にある DHCP リレークライアント。

- APIC から既存の DHCP ポリシーをインポートしています。
- グローバルファブリックアクセスポリシーでの DHCP リレーポリシーの設定はサポートされていません
- 同じ DHCP リレーポリシー内の複数の DHCP サーバと EPG。

同じ DHCP リレーポリシーで複数のプロバイダを設定する場合は、それぞれ異なる EPGs または外部 EPGs にする必要があります。

DHCP リレー ポリシーの作成

このセクションでは、DHCP リレー ポリシーの作成方法について説明します。



- (注) ブリッジドメインに DHCP ポリシーを割り当て、ブリッジドメインを1つ以上のサイトに展開した後で DHCP ポリシーに変更を加えた場合、DHCP ポリシーの変更が各サイトの APIC で更新されるように、ブリッジドメインを再展開する必要があります。

始める前に

次のものがが必要です。

- 環境でセットアップして設定された DHCP サーバー。
- DHCP サーバーがアプリケーション EPG の一部である場合には、その EPG が Nexus Dashboard Orchestrator ですでに作成されている必要があります。
- DHCP サーバーがファブリックの外部にある場合には、DHCP サーバーにアクセスするために使用される L3Out に関連付けられた外部 EPG が、すでに作成されている必要があります。

-
- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] を選択します。
- ステップ 3** メインペインの右上で[ポリシー追加 (Add Policy)] > [DHCP ポリシーの作成 (Creating DHCP Policy)] を選択します。
- これは、[DHCP の追加] 設定画面を開きます。
- ステップ 4** [名前 (Name)] フィールドにポリシーの名前を入力します。
- ステップ 5** [テナントの選択] ドロップダウンから、DHCP サーバを含むテナントを選択します。
- ステップ 6** (オプション) [説明] フィールドに、このポリシーの説明を入力します。
- ステップ 7** タイプに対して、リレーを選択します。

ステップ 8 [+プロバイダ] をクリックします。

ステップ 9 プロバイダ タイプを選択します。

リレー ポリシーを追加するときには、次の 2 つのタイプのうちの 1 つを選択できます。

- アプリケーション EPG—エンドポイントとして追加する DHCP サーバを含む特定のアプリケーション EPG を指定します。
- L3 外部ネットワーク—DHCP サーバーへのアクセスに使用される L3Out に関連付けられた外部 EPG を指定します。

(注) Orchestrator をサイトにまだ展開していない場合でも、Orchestrator で作成され、指定したテナントに割り当てられている EPG または外部 EPG を選択できます。展開されていない EPG を選択した場合でも、DHCP リレー構成を完了することができますが、リレーが使用可能になる前に EPG を展開する必要があります。

ステップ 10 ドロップダウンメニューから、EPG または外部 EPG を選択します。

ステップ 11 [DHCP サーバアドレス] フィールドに、DHCP サーバの IP アドレスを入力します。

ステップ 12 [保存 (Save)] をクリックして、プロバイダを追加します。

ステップ 13 (オプション) 追加プロバイダがあれば、それを加えます。

追加のそれぞれの DHCP サーバに対して手順 9~12 を繰り返します。

ステップ 14 [保存 (Save)] をクリックして DHCP リレー ポリシーを保存します。

DHCP オプションポリシーの作成

このセクションでは、DHCP オプションポリシーの作成方法について説明します。DHCP オプションは、DHCP サーバとクライアントが交換するメッセージの末尾に追加され、DHCP サーバに追加の設定情報を提供するために使用されます。各 DHCP オプションには、オプションポリシーを追加するときに指定する必要がある特定のコードがあります。DHCP オプションとコードの完全なリストの場合は、[RFC 2132](#) を参照してください。

始める前に

次のものをあらかじめ設定しておく必要があります。

- 環境でセットアップして設定された DHCP サーバー。
- Nexus Dashboard Orchestrator ですでに作成してある DHCP サーバを含む EPG。
- [DHCP リレー ポリシーの作成 \(203 ページ\)](#) の説明に従って作成された DHCP リレー ポリシー。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

- ステップ 2** 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] を選択します。
- ステップ 3** メイン ペインの右上で[ポリシー追加 (Add Policy)] > > [DHCP ポリシーの作成 (Creating DHCP Policy)] を選択します。
- これは、[DHCP の追加] 設定画面を開きます。
- ステップ 4** [名前 (Name)] フィールドにポリシーの名前を入力します。
- これは、作成しているポリシーの名前であり、特定の DHCP オプションの名前ではありません。各ポリシーには、複数の DHCP オプションが含まれる場合があります。
- ステップ 5** [テナントの選択] ドロップダウンから、DHCP サーバを含むテナントを選択します。
- ステップ 6** (オプション) [説明] フィールドに、このポリシーの説明を入力します。
- ステップ 7** [タイプ] に対して [オプション] を選択します。
- ステップ 8** [+オプション (+Options)] をクリックします。
- ステップ 9** オプションの名前を指定します。
- 技術的には要求されていませんが、RFC 2132 にリストされたオプションに同じ名前を使用することをお勧めします。
- たとえば、ネーム サーバが挙げられます。
- ステップ 10** オプションの ID を指定します。
- RFC 2132 にリストされているとおり、オプション コードを提供する必要があります。
- たとえば、ネーム サーバ オプションに対して 5 が挙げられます。
- ステップ 11** オプションのデータを指定します。
- オプションが値を要求した場合はそれを指定します。
- たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。
- ステップ 12** [データ] フィールドの隣のチェックマークをクリックして、オプションを保存します。
- ステップ 13** (オプション) 追加オプションを加えるための手順を繰り返します。
- ステップ 14** [保存 (Save)] をクリックして DHCP オプション ポリシーを保存します。

DHCP ポリシーの割り当て

この項では、ブリッジドメインを作成する方法について説明します。



- (注) ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジドメインを 1 つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジドメインを再展開する必要があります。

始める前に

次のものをあらかじめ設定しておく必要があります。

- [DHCP リレー ポリシーの作成 \(203 ページ\)](#) の説明に従って、DHCP リレー ポリシー。
- (オプション) [DHCP オプションポリシーの作成 \(204 ページ\)](#) の説明に従って、DHCP オプション ポリシー。
- [スキーマとテンプレートの作成 \(24 ページ\)](#) 章の説明に従って、DHCP ポリシーに割り当てられたブリッジ ドメイン。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 ブリッジドメインが定義されているスキーマを選択します。

ステップ 4 [[ブリッジドメイン (Bridge domain)] エリアまで下にスクロールし、ブリッジドメインを選択します。

ステップ 5 右側のサイドバーで、下にスクロールして、[DHCP ポリシー (DHCP Policy)] オプションチェックボックスをオンにします。

ステップ 6 [DHCP リレーポリシー (DHCP Relay policy)] ドロップダウンから、この BD に割り当てる DHCP ポリシーを選択します。

ステップ 7 (オプション)[DHCP オプションポリシー (DHCP Option policy)] ドロップダウンから、オプションポリシーを選択します。

DHCP オプション ポリシーは、DHCP リレーに渡す追加のオプションを提供します。詳細については、[DHCP オプションポリシーの作成 \(204 ページ\)](#) を参照してください。

ステップ 8 リレー経由でDHCPサーバにアクセスする必要があるすべてのEPGにブリッジドメインを割り当てます。

DHCP リレー コントラクトの作成

DHCP パケットはコントラクトによりフィルタリングされませんが、VRF 内および VRF 間でルーティング情報を伝播するには、多くの場合コントラクトが必要です。DHCP パケットはフィルタリングされませんが、クライアント EPG と DHCP リレー ポリシーでプロバイダとして設定された EPG の間のコントラクトを設定することをお勧めします。

このセクションでは、DHCP サーバーを含む EPG と、リレーを使用する必要があるエンドポイントを含む EPG の間でコントラクトを作成する方法について説明します。DHCP ポリシーを作成してブリッジドメインに、また、ブリッジドメインをクライアントの EPG にすでに割り当てている場合でも、クライアントからサーバーへの通信を可能にするルートのプログラミングを有効にするには、コントラクトを作成して割り当てる必要があります。

始める前に

次のものをあらかじめ設定しておく必要があります。

- [DHCP リレー ポリシーの作成 \(203 ページ\)](#) の説明に従って、DHCP リレー ポリシー。
- (オプション) [DHCP オプション ポリシーの作成 \(204 ページ\)](#) の説明に従って、DHCP オプション ポリシー。
- [DHCP ポリシーの割り当て \(205 ページ\)](#) の説明に従って、DHCP ポリシーに割り当てられたブリッジドメイン。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[スキーマ(Schemas)]** を選択します。

ステップ 3 コントラクトを作成したいスキーマを選択します。

ステップ 4 コントラクトを作成します。

DHCP パケットはコントラクトによってフィルタリングされていないため、特定のフィルタは必要ありませんが、有効なコントラクトが作成され、割り当てられて、適切な BD およびルート展開を保證する必要があります。

- a) **[コントラクト (Contracts)]** エリアまで下方にスクロールし、+ をクリックして、コントラクトを作成します。
- b) 右のプロパティのサイドバーでは、コントラクトの**表示名**を指定します。
- c) **[範囲 (Scope)]** ドロップダウンから、適切な範囲を選択します。

DHCP サーバ EPG とアプリケーション EPG は同じテナントになければならないため、次のうちの1つを選択できます。

- `vrf`。両方の EPG が同じ VRF にある場合
- テナント。EPG が異なる VRF にある場合

- d) **[両方向に適用 (Apply Both Directions)]** ノブをオンのままにすることができます。

ステップ 5 DHCP リレー EPG にコントラクトを割り当てます。

- a) EPG が配置されているテンプレートを参照します。
- b) DDHCP サーバが常駐する EPG または外部 EPG を選択します。

これは、DHCP リレー ポリシーを作成するときに選択したのと同じ EPG です。

- c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
- d) 作成したコントラクトとそのタイプのプロバイダを選択します。

ステップ 6 エンドポイントが DHCP リレー アクセスを必要とするアプリケーション EPG にコントラクトを割り当てます。

- a) アプリケーション EPG が配置されているテンプレートを参照します。
- b) アプリケーション EPG を選択します。
- c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。

- d) 作成したコントラクトとそのタイプのコンシューマを選択します。

APIC での DHCP リレー ポリシーの確認

ここでは、Nexus Dashboard を使用して作成および展開した DHCP リレーポリシーが各サイトの APIC に正しくプッシュされることを確認する方法について説明します。作成する DHCP ポリシーは、ポリシーが関連付けられているブリッジドメインがサイトに展開しているときに、APIC にプッシュされます。

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 上部のナビゲーションバーから、[テナント(tenant)] > <テナント名>を選択します。

DHCP ポリシーを展開したテナントを選択します。

ステップ 3 APIC で DHCP リレー ポリシーが設定されていることを確認します。

左側のツリー ビューで、<テナント名>> **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **リレー ポリシー (Relay policies)** に移動します。次に、設定した DHCP リレー ポリシーが作成されていることを確認します。

ステップ 4 DHCP オプション ポリシーが APIC で設定されていることを確認します。

DHCP オプション ポリシーを設定していない場合は、この手順をスキップできます。

左側のツリー ビューで、<テナント名>> **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **オプション ポリシー (Option Policies)** に移動します。次に、設定した DHCP オプション ポリシーが作成されていることを確認します。

ステップ 5 DHCP ポリシーがブリッジ ドメインに正しく関連付けられていることを確認します。

左側のツリー ビューで、<テナント名>> **ネットワーク** > **ブリッジ ドメイン** > <ブリッジ ドメイン名>> **DHCP リレー ラベル** に移動します。展開されたブリッジ ドメインにも DHCP ポリシーが関連付けられていることを確認します。

既存の DHCP ポリシーの編集または削除

このセクションでは、DHCP リレーまたはオプションポリシーを編集または削除する方法について説明します。



- (注)
- ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジドメインを1つ以上のサイトに展開した場合は、DHCP ポリシーの変更が各サイトの APIC で更新されるように再展開する必要があります。
 - 1つ以上のブリッジドメインに関連付けられているポリシーを削除することはできません。最初に、すべてのブリッジドメインからポリシーの割り当てを解除する必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから [ポリシー] を選択します。

ステップ 3 DHCP ポリシーの横にある [アクション] メニューをクリックし、[編集 (Edit)] または [削除 (Delete)] を選択します。



第 19 章

EPG 優先グループ

- [EPG 優先グループ \(211 ページ\)](#)
- [優先グループに対する EPG の設定 \(213 ページ\)](#)

EPG 優先グループ

デフォルトでは、Multi-Site アーキテクチャは EPG 間でコントラクトが設定されている場合のみ、EPG 間の通信を許可します。EPG 間にコントラクトがない場合は、EPG 間の通信は明示的に無効になります。優先グループ (PG) 機能を使用すると、同じ VRF の一部である複数の EPG を指定して、コントラクトを作成する必要なく、それらの間の完全な通信を可能にすることができます。

優先グループ対コントラクト

コントラクト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施行には 2 種類あります。

- **EPG を含む** - 優先グループのメンバーである EPG は、コントラクトなしでグループ内の他のすべての EPG と自由に通信できます。通信は、`source-any-destination-any-permit` のデフォルトルールと適切な Multi-Site 変換に基づいています。
- **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コントラクトが必要です。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。

コントラクト優先グループ機能を使用すると、拡張 VRF コンテキストのサイト間での EPG 間の通信をより詳細に制御し、設定を容易にすることができます。拡張 VRF の 2 つ以上の EPG がオープン通信を要求する一方で、他は制限された通信しかもてない場合、コントラクト優先グループとフィルタ付きのコントラクトの組み合わせを設定し、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コントラクトがある場合にのみ、他の EPG と通信できます。

拡張 対 シャドウ

複数のサイトの EPG が同じコントラクト優先グループの一部になるように構成されている場合、Nexus Dashboard Orchestrator は他のサイトに各サイトの EPG のシャドウを作成して、EPG からサイト間接続を正しく変換およびプログラムします。次に、コントラクト優先グループポリシーコンストラクトが、EPG 間通信の実際の EPG とシャドウ EPG の間の各サイトに適用されます。

たとえば、Site1 のウェブサービス EPG1 と Site2 のアプリサービス EPG2 がコントラクト優先グループに追加される場合を考察します。次に、EPG1 が EPG2 にアクセスする場合は、最初にサイト 2 のシャドウ EPG1 に変換され、次にコントラクト優先グループを使用して EPG2 と通信できるようになります。適切な BD は、その下の EPG がコントラクト優先グループの一部である場合、拡張されるか、シャドウされます。

VRF 優先グループ設定

優先グループを APIC で直接設定する場合は、個々の EPG で PG メンバーシップを有効にする前に、まず VRF で設定を明示的に有効にする必要があります。VRF の PG 設定が無効になっている場合、EPG はその VRF の優先グループの一部であっても、コントラクトなしでは通信できません。

一方、Nexus Dashboard Orchestrator では、GUI で VRF の PG 設定を管理することはできませんが、代わりに次のように動的に設定を調整します。

- NDO から VRF を作成および管理する場合、NDO は、その VRF に属する EPG が優先グループの一部であるかどうかに基づいて、VRF PG 値を動的に有効または無効にします。
つまり、1 つ以上の EPG を優先グループに追加すると、NDO は VRF の PG 設定を自動的に有効にします。優先グループから最後の EPG を削除すると、NDO は VRF フラグを無効にします。
- VRF で PG オプションを永続的に有効にするには、最初に APIC で VRF の PG を直接有効にしてから、その VRF を NDO にインポートします。
VRF の優先グループからすべての EPG を削除しても、NDO は設定を保持し、自動的に無効にしません。
- 最初に PG 設定を変更せずに APIC から VRF をインポートすると、NDO はオブジェクトを NDO から作成されたかのように管理し、EPG メンバーシップに基づいて PG 設定を動的に上書きします。

制限事項

優先グループは、サイト間 L3Out 外部 EPG ではサポートされません。

優先グループに対する EPG の設定

始める前に

スキーマ テンプレートに 1 つ以上の EPG を追加する必要があります。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] を選択します。
- ステップ 3 変更するスキーマをクリックします。
- ステップ 4 優先グループの一部として、スキーマで 1 つ以上の EPG を設定します。

(注) APIC のいずれかに既存の優先グループがあり、その優先グループから Nexus Dashboard Orchestrator に EPG をインポートすることを計画している場合は、グループ内のすべての EPG をインポートする必要があります。一部の EPG が Nexus Dashboard Orchestrator によって管理され、一部がローカル APIC によって管理される優先グループを設定することはできません。

単一の EPG を追加または削除するには:

- a) EPG を選択します。
- b) 右側のプロパティ バーで、[優先グループに含める] チェックボックスをオンまたはオフにします。
- c) メイン ウィンドウの右上の隅にある [保存] をクリックします。

複数の EPG を一度に追加または削除するには:

- a) [アプリケーション プロファイル] タブの右上隅の **SELECT** をクリックします。
- b) 1 つまたは複数の EPG をクリックして選択するか、[すべて選択] をクリックしてすべての EPG を選択します。
- c) [アプリケーション プロファイル (Application Profile)] タブの右上隅の ... をクリックして、[優先グループへの EPG の追加] または [優先グループからの EPG の削除] を選択します。
- d) メイン ウィンドウの右上の隅にある [保存] をクリックします。

次のタスク

VRF を選択し、右側のプロパティ サイドバーで **PREFERRED GROUP EPGS** リストを確認すると、優先グループの一部として構成されている EPG の完全なリストを表示できます。



第 20 章

サイト内 L3Out

- [サイト間 L3Out の概要 \(215 ページ\)](#)
- [サイト内 L3Out のガイドラインと制約事項 \(216 ページ\)](#)
- [外部 TEP プールの設定 \(218 ページ\)](#)
- [サイト間 L3Out および VRF の作成またはインポート \(218 ページ\)](#)
- [サイト間 L3Out を使用するための外部 EPG の設定 \(221 ページ\)](#)
- [サイト間 L3Out のコントラクトの作成 \(224 ページ\)](#)
- [使用例 \(227 ページ\)](#)

サイト間 L3Out の概要

リリース 2.2(1) 以前、Nexus Dashboard Orchestrator により管理される各サイトでは、トラフィックをファブリックの外にルートするために設定された固有のローカル L3Out が必要で、それによりしばしば 1 つのサイトのエンドポイントと別のサイトの L3Out に接続されたサービス (ファイアウォール、サーバロードバランサー、またはメインフレーム) の間のコミュニケーションの欠如を導くことができました。

リリース 2.2(1) は、1 つのサイトにあるエンドポイントが、外部ネットワーク、メインフレーム、またはサービス ノードなどのリモート L3Out を通じて到達可能なエンティティとの接続を確立する多くのシナリオを有効にする機能を追加します。

このような要素として、次のものが挙げられます。

- **サイト間の L3Out** : 別のサイトの L3Out を使用した 1 つのサイトのアプリケーション EPG のエンドポイント。
- **サイト間中継ルーティング** : 異なるサイトに展開された L3Out (同じ VRF の両方の L3Out) の背後に接続されたエンティティ (エンドポイント、ネットワークデバイス、サービス ノードなど) 間の通信を確立します。
- **サイト間 L3Out の共有サービス** : リモート E3Out へのアプリケーション EPG またはサイト間中継ルーティング。

次のセクションは、サイト間 L3Out の使用例の実装に必要なオブジェクトを作成するために実行できる一般的な GUI 手順に分かれています。その後、サポートされる各使用例のシナリオに固有の概要とワークフローを示します。



- (注) 「サイト間 L3Out」という用語は、リモートサイトの L3Out 接続を介して到達可能な外部リソースへの通信を可能にする機能を指します。ただし、このドキュメントでは、この用語は特定のリモート L3Out オブジェクトを示すためにも使用されることがあります。

サイト内 L3Out のガイドラインと制約事項

サイト間 L3Out を構成するときは、次のことを考慮する必要があります。

- サイト間 L3Out は IPv4 と IPv6 に対してサポートされています。
- サイト間 L3Out では、Multi-Site トポロジ内のサイト間で常に確立される BGP eVPN セッションに加えて、サイト間 L3Out 機能をサポートするために MP BGP VPNv4 (または VPNv6) セッションが作成されます。
- リリース 2.2(1) 以前のリリースからアップグレードしている場合、サイトローカルレベルの既存の外部 EPG から L3Out への関連付けは保持されます。さらに、Nexus Dashboard Orchestrator は L3Out の作成とテンプレートレベルでの外部 EPG との関連付けをサポートするようになりました。

スキーマテンプレートで新しい L3Out を作成し、既存の外部 EPG に関連付ける場合：

- L3Out が APIC ですでに定義されている L3Out と同じ名前の場合、Orchestrator その L3Out の所有権を取得しますが、L3Out ノードプロファイル、インターフェースプロファイル、プロトコル設定、またはルート制御設定の構成を管理しません。



- (注) L3Out が APIC にすでに存在する場合は、NDO から同じ名前の新しい L3Out を作成するのではなく、関連付けられた外部 EPG とともに Nexus Dashboard Orchestrator にインポートすることをお勧めします。

次に、Orchestrator からこの L3Out を削除することになると、それは Orchestrator により管理されなくなりますが、以前から存在する L3Out の構成は APIC に保存されます。

- L3Out が L3Out で定義された APIC とは異なる名前がある場合、外部 EPG は、APIC で定義された L3Out から削除され、Orchestrator で定義された L3Out に追加されます。これが APIC で定義された L3Out での唯一の外部 EPG である場合、これにより設定が境界リーフから削除され、トラフィックに影響を与える可能性があります。

- リリース 2.2(1) より前のリリースにダウングレードすることを選択した場合、Orchestrator NDO で作成された L3Out はテンプレートに存在しなくなるため、外部 EPG と L3Out 間のテンプレート レベルの関連付けは削除されます。この場合、サイト ローカル レベルで、外部 EPG と L3Out の関連付けを手動で再構成する必要があります。ダウングレード中、サイトローカルの関連付けは保持されます。
- これで、1つのサイトのブリッジドメインを別のサイトの L3Out に関連付けることができますが、両方が同じ VRF にある必要があります。

この関連付けはサイトローカルレベルで実行され、リモート L3Out から BD サブネットをアドバタイズし、ローカル L3Out に障害が発生した場合でも BD へのインバウンドトラフィックを維持できるようにするために必要です。
- サイト間 L3Out に関連付けられた VRF のポリシー制御施行方向は、デフォルトの入力モードで構成されたままにする必要があります。
- 次のシナリオは、サイト間 L3Out およびリモートリーフ (RL) ではサポートされていません。
 - 別々のサイトに関連付けられた RL ペアにデプロイされた L3Out 間のトランジットルーティング
 - リモートサイトに関連付けられた RL ペアに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント
 - リモートサイトに関連付けられた RL ペアに展開された L3Out と通信するローカルサイトに接続されたエンドポイント
 - リモートサイトに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント
- 次の他の機能は、ACI Multi-Site のサイト間 L3Out ではサポートされていません。
 - 別のサイト L3Out を介して外部ソースからマルチキャストを受信するサイト内のマルチキャストレシーバー。サイトで外部ソースから受信したマルチキャストが他のサイトに送信されることはありません。サイトのレシーバーが外部ソースからマルチキャストを受信する場合、ローカルの L3Out で受信する必要があります。
 - PIM-SM Any Source Multicast (ASM) を使用して外部レシーバーにマルチキャストを送信する内部マルチキャストソース。内部マルチキャストソースは、ローカル L3Out から外部ランデブーポイント (RP) に到達できる必要があります
 - GOLF
 - 外部 EPG の優先グループ

外部 TEP プールの設定

サイト間 L3Out には、各ポッドの境界リーフ スイッチに外部 TEP アドレスが必要です。外部 TEP プールがすでに設定されている場合(たとえば、リモートリーフなどの別の機能のために)は、同じプールを使用できます。既存の TEP プールは Nexus Dashboard Orchestrator に継承され、インフラストラクチャ設定の一部として GUI に表示されます。それ以外の場合は、この項で説明されているように、GUI で TEP プールを追加できます。



(注) すべてのポッドに一意的な TEP プールを割り当てる必要があり、ファブリック内の他の TEP プールと重複しないようにする必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。

ステップ 4 左側のサイドバーで、設定するサイトを選択します。

ステップ 5 メイン ウィンドウで、サイト内のポッドをクリックします。

ステップ 6 右側のサイドバーで、[+ TEP プールを追加 (+Add TEP Pool)] をクリックします。

ステップ 7 [TEP プールの追加 (Add TEP pool)] ウィンドウで、そのサイトに対して設定する外部 TEP プールを指定します。

(注) 追加しようとしている TEP プールが他の TEP プールまたはファブリックアドレスと重複していないことを確認する必要があります。

ステップ 8 このプロセスを、サイト間の L3Outs を使用する予定のサイトおよびポッドごとに繰り返します。

サイト間 L3Out および VRF の作成またはインポート

ここでは、L3Out を作成し、それを Orchestrator GUI で VRF に関連付ける方法について説明します。これは APIC サイトにプッシュされるか、または APIC サイトの 1 つから既存の L3Out をインポートします。次に、この L3Out を外部 EPG に関連付け、その外部 EPG を使用して特定のサイト間 L3Out の使用例を設定します。



(注) L3Out に割り当てる VRF は、任意のテンプレートまたはスキーマにすることができますが、L3Out と同じテナントに存在する必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 [スキーマ (schema)] を選択し、VRF と L3Out を作成またはインポートするテンプレートを選択します。

1 つのサイトに関連付けられているテンプレートで L3Out を作成することを推奨します。この場合、そのサイトでのみ L3Out が作成されます。

または、複数のサイトに関連付けられているテンプレートで L3Out を作成することもできます。この場合、すべてのサイトで同じ名前でも L3Out が作成されます。これにより、この章で後述するように、いくつかの機能制限が生じる可能性があります。

ステップ 4 新しい VRF と L3Out を作成します。

既存の L3Out をインポートする場合は、この手順をスキップします。

(注) Orchestrator で L3Out オブジェクトを作成し、それを APIC にプッシュすることはできますが、L3Out の物理設定は APIC で実行する必要があります。

a) **[VRF]** エリアまで下にスクロールし、+ アイコンをクリックして新しい VRF を追加します。

L3Out に使用する予定の VRF がすでにある場合は、このサブステップをスキップします。

右側のサイドバーで、VRF の名前を入力します (例: vrf-l3out)。

b) **[L3Out]** 領域まで下にスクロールし、+ アイコンをクリックして新しい L3Out を追加します。

右側のスライダで、必要な情報を入力します。

c) L3Out の名前を指定します (例: l3out-intersite)。

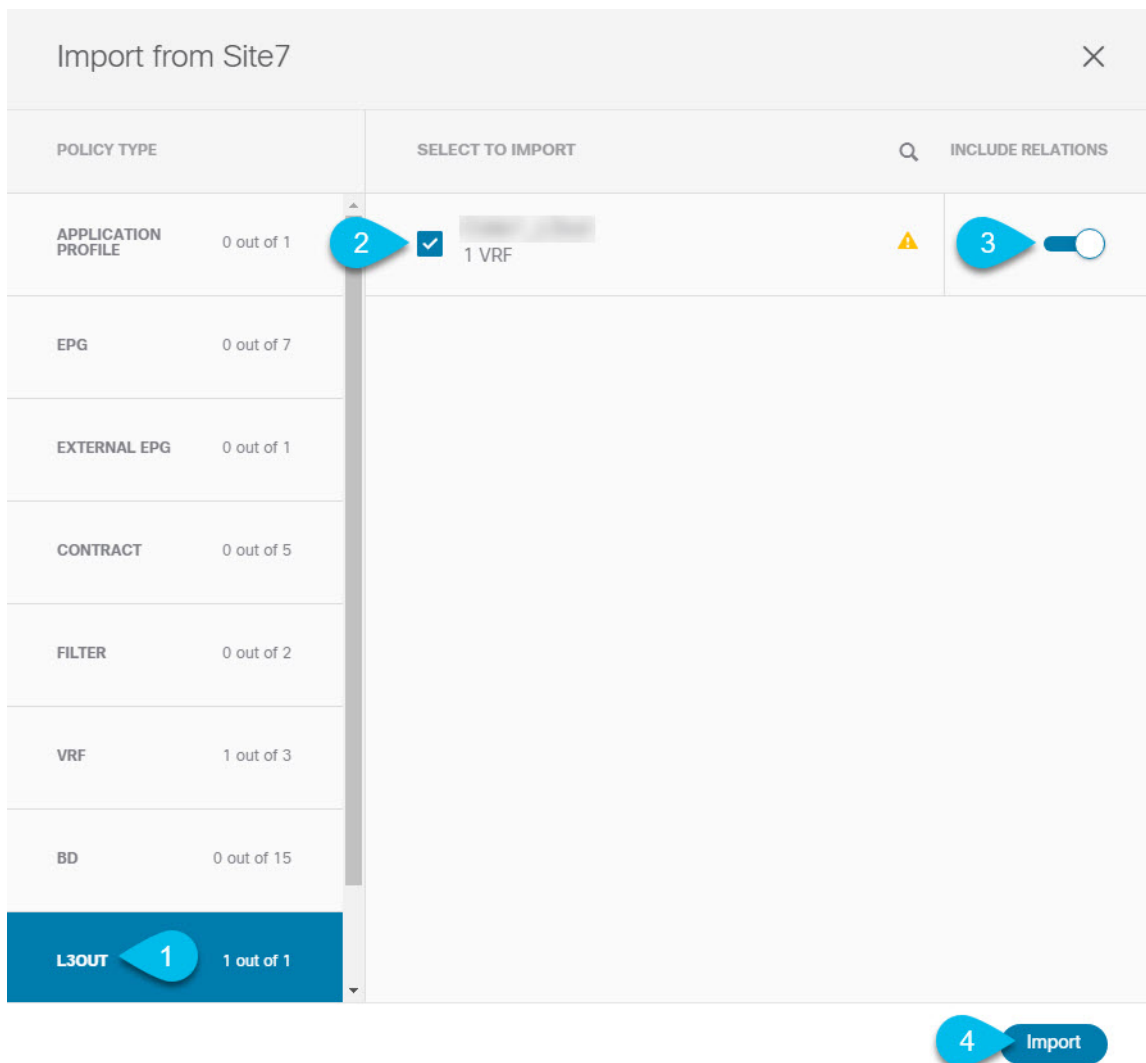
d) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、VRF を選択します。

最初のサブステップで作成した VRF を選択するか、既存の VRF を選択します。

ステップ 5 既存の VRF および L3Out をインポートします。

前の手順で新しい L3Out を作成した場合は、この手順をスキップします。

メイン ウィンドウ ペインの **[インポート (Import)]** をクリックして、



- メインテンプレートビューの上部で、[インポート (Import)] をクリックします。
- L3Out をインポートするサイトを選択します。
- [インポート (Import)] ウィンドウの [ポリシー タイプ(Policy Type)] メニューで、[L3Out] を選択します。
- インポートする L3Out をチェックします。

デフォルトでは、L3Outをインポートすると、対応するVRFもインポートされます。これは、サイト固有のテンプレートでL3Outをインポートする場合、通常は複数のサイトに関連付けられた拡張テンプレートでVRFを定義するため、望ましくない場合があります。この場合、L3Outをインポートする前に [Include Relationships] オプションを無効にします。この場合、インポート後にL3Outを正しいVRFに再マッピングする必要もあります。

- [インポート (Import)] をクリックします。

- f) L3Outのみをインポートした場合は、テンプレートビューでそれを選択し、適切なVRFに関連付けます。

サイト間 L3Out を使用するための外部 EPG の設定

このセクションでは、サイト間L3Outと関連付ける外部EPGの作成方法について説明します。その後、この外部EPGとコントラクトを使用すれば、あるサイトのエンドポイント用の特定のユースケースを設定し、別のサイトのL3Outを使用することができます。

始める前に

L3Outを作成し、[サイト間L3OutおよびVRFの作成またはインポート \(218ページ\)](#) に説明されている方法でVRFと関連付けます。

ステップ1 外部 EPG を作成するテンプレートを選択します。

複数のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、それらすべてのサイト上で作成されます。これは、外部 EPG の L3Out が WAN などの一連の共通外部リソースへのアクセスを提供する場合に推奨されます。

単一のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、そのサイト内でのみ作成されます。これは、外部 EPG の L3Out がそのサイトからのみアクセス可能な外部リソースへのアクセスを提供する場合に推奨されます。

ステップ2 [外部 EPG (External EPG)] エリアまで下方にスクロールして、+アイコンをクリックして外部 EPG を追加します。

右側のスライダで、必要な情報を入力します。

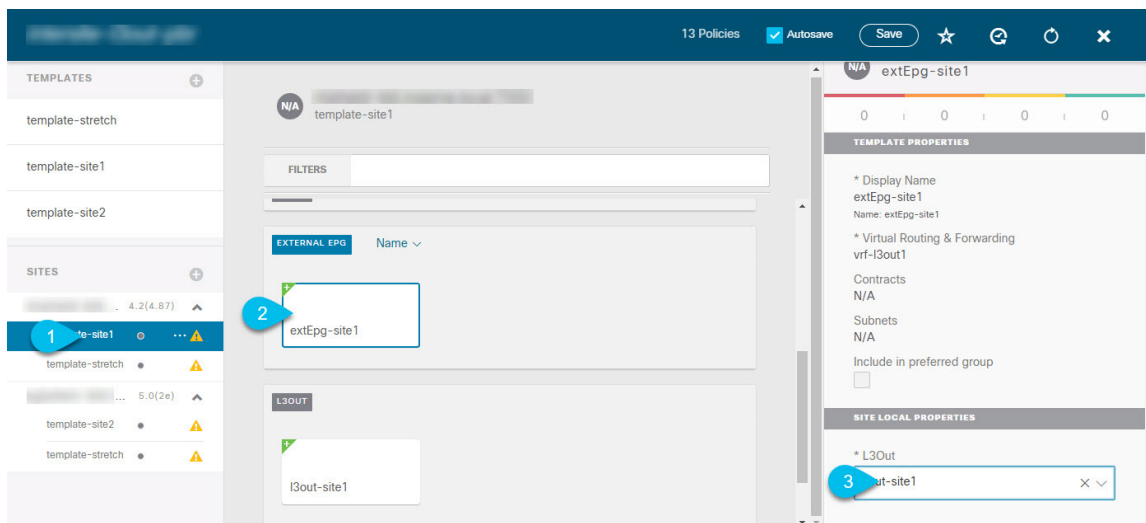
- 外部 EPG の名前を入力します。たとえば [eepg-intersite-l3out] のようにします。
- [仮想ルーティングと転送 (Virtual Routing & Forwarding)] ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。

ステップ3 外部 EPG を L3Out にマッピングします。

サイトレベルまたはテンプレートレベルで、外部 EPG を L3Out にマッピングできます。通常、各サイトはローカル L3Out を一意の名前で定義するため、外部 EPG 自体が拡張されているかどうかに関係なく、外部 EPG を各サイト固有の L3Out に選択的にマッピングできます。それで、サイトレベルでマッピングを作成することをお勧めします。

L3Out をサイトローカル レベルで外部 EPG に関連付けるには、次の手順に従います。

サイト間 L3Out を使用するための外部 EPG の設定

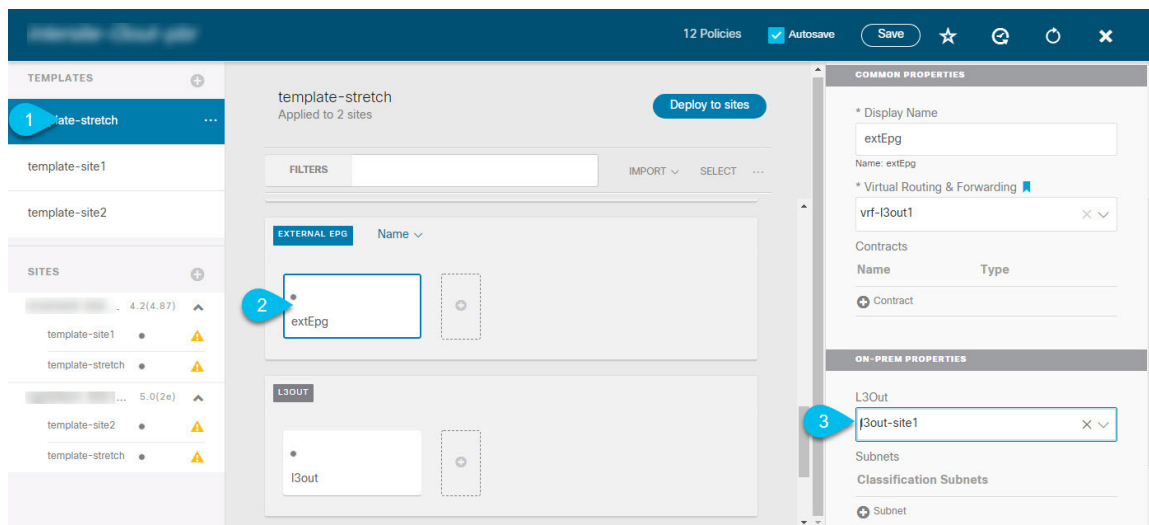


- スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。
- [外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。
- 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

この場合、APIC で管理されている L3Out と、オーケストレーションで管理されている L3Out の両方が選択できます。前のセクションでこの目的のため特に作成した L3Out、またはサイトの APIC 内にすでにある L3Out のいずれかを選択します。

サイト レベルまたはテンプレート レベルで、外部 EPG を L3Out にマッピングできます。これにより、複数のサイトで同じ L3Out 名が定義されている展開での設定が容易になりますが、マルチサイトドメインやおよび外部ルーテッドネットワークの一部であるファブリック間で確立できる接続タイプの柔軟性が低下するため、このアプローチは推奨されません。たとえば、特定の BD のサブネットがアダプタイズされる場所を制御することはできません。これは、L3Out に BD をマッピングすると、すべての L3Out が同じ名前を持つため、すべてのサイトのすべての L3Out から BD サブネットがアダプタイズされるためです。

テンプレート レベルで L3Out を外部 EPG に関連付けるには、次の手順を実行します。



- スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。
- [外部 EPG (External EPG)] エリアまで下方にスクロールして、外部 EPG を選択します。
- 右サイドバーで、[L3Out] ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

また、テンプレート レベルで L3Out に最初に関連付けられた外部 EPG の設定を、サイトレベルのマッピングに移行することもできます。これを行うには、外部 EPG の VRF 関連付けを削除し、外部 EPG を同じ VRF に再び関連付け、それからサイトレベルで L3Outs をマッピングします。このプロセスがテンプレートを展開する前に一度に完了しておけば、APIC 側で実際に変更が適用されないため、新しい設定をプッシュする際にトラフィックに影響はありません。

ステップ 4 外部 EPG に 1 つ以上のサブネットを設定します。

- 外部 EPG を選択します。
- 右側のサイドバーで、[+ サブネットを追加 (+Add Subnet)] をクリックします。
- [サブネットを追加 (Add Subnet)] ウィンドウで、分類サブネットと必要なオプションを入力します。

設定するプレフィックスとオプションは、使用例によって異なります。

- 着信トラフィックを外部 EPG に属するものとして分類するには、指定したプレフィックスの [外部 EPG の外部サブネット (External Subnets for External EPG)] フラグを選択します。使用例に応じて、内部 EPG またはリモート L3Out 経由で到達可能な外部ネットワーク ドメインとの契約を適用できます。
- この L3Out から (同じサイトまたはリモートサイト内の) 別の L3Out から学習した外部プレフィックスをアドバタイズするには、指定したプレフィックスの [エクスポートルート制御 (Export Route Control)] フラグを選択します。0.0.0.0/0 プレフィックスを指定する場合は、L3Out からのすべてのプレフィックスをアドバタイズするために [集約エクスポート (Aggregate Export)] フラグを選択できます。[集約エクスポート (Aggregate Export)] フラグが有効になっていない場合、デフォルトルートの 0.0.0.0/0 だけがアドバタイズされます (ボーダーリーフ ノードのルーティング テーブルに存在する場合)。

- 外部ネットワークから受信した特定のルートを除くには、指定したプレフィックスの[ルート制御のインポート (Import Route Control)] フラグを選択します。0.0.0.0/0 を指定する場合は、[集約インポート (Aggregate Import)] オプションを選択することもできます。

これは、BGP を外部ルータとピアリングする場合にのみ可能であることに注意してください。

- 異なるVRFにルートをリークするには、[共有ルート制御 (Shared Route Control)] と関連する [集約共有ルート (Aggregate Shared Routes)] フラグ、および [共有セキュリティ インポート (Shared Security Import)] フラグを選択します。これらのオプションは、VRF 間共有 L3Out および VRF 間サイト間中継ルーティングの特定の使用例に必要です。

サイト間 L3Out のコントラクトの作成

ここでは、サイトに展開されたアプリケーション EPG と、別のサイトの L3Out に関連付けられた外部 EPG（サイト間 L3Out 機能）との間の通信を可能にするために使用するフィルタとコントラクトを作成する方法について説明します。

ステップ 1 コントラクトとフィルタを作成するためのテンプレートを選択します。

L3Out、VRF、および外部 EPG を作成したのと同じスキーマとテンプレートを使用できます。または、別のスキーマとテンプレートを選択することもできます。

コントラクトは異なるサイトに展開されたオブジェクト（EPG および外部 EPG）に適用されるため、複数のサイトに関連付けられたテンプレートで定義することを推奨します。ただし、これは必須ではありません。コントラクトとフィルタが Site1 のローカルオブジェクトとしてのみ定義されている場合でも、Site2 のローカル EPG または外部 EPG がそのコントラクトを消費または提供する必要がある場合、NDO はリモート Site2 に対応するシャドウオブジェクトを作成します。。

ステップ 2 フィルタを作成します。

- a) **[Filter (フィルタ)]** エリアまでスクロールし、**[+]** をクリックしてフィルタを作成します。
- b) 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。
- c) 右側のペインで、**[+ エントリ (+ Entry)]** をクリックします。

ステップ 3 フィルタの詳細を入力します。

Add Entry ×

COMMON PROPERTIES

Name
icmp 1

Description

Ether Type
ip 2

IP Protocol
icmp

Destination port range from
unspecified

Destination port range to
unspecified 3

ON-PREM PROPERTIES

Match only fragments
 stateful

ARP flag
unspecified × ▼

Source port range from
unspecified ▼

Source port range to
unspecified ▼

TCP session rules
unspecified × ▼

4 Save

- a) フィルタの [名前 (Name)] を指定します。
- b) [イーサertype (Ether Type)] を選択します。

たとえば [ip] です。

- c) **[IP プロトコル (IP Protocol)]** を選択します。

たとえば [icmp] です。

- d) 他のプロパティは未指定のままにします。
- e) **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ4 コントラクトの作成

- a) 中央ペインで、**[コントラクト (Contracts)]** エリアまで下方にスクロールし、**[+]** をクリックして、コントラクトを作成します。
- b) 右側のペインで、コントラクトの **[表示名 (Display Name)]** を入力します。
- c) コントラクトの適切な **[範囲 (Scope)]** を選択します。

サイト間 L3Out の別の VRF にある共有サービス エンドポイントを設定する場合には、その範囲のテナントを選択する必要があります。それ以外の場合、両方が同じ VRF 内にある場合は、範囲を `vrf` に設定できます。

- d) コンシューマからプロバイダーへの方向とプロバイダーからコンシューマへの方向の両方に同じフィルタを適用する場合は、**[両方向に適用 (Apply both directions)]** ノブを切り替えます。

このオプションを有効にした場合は、フィルタを 1 回だけ指定することが必要となり、両方向のトラフィックに適用されます。このオプションを無効のままにした場合は、各方向に1つずつ、2セットのフィルタ チェーンを指定する必要があります。

ステップ5 コントラクトにフィルタを割り当てる

- a) 右側のペインで、**[フィルタ チェーン (Filter Chain)]** 領域までスクロールし、**[+ フィルタ (+ Filter)]** をクリックしてフィルタをコントラクトに追加します。

コントラクトで **[両方向に適用 (Apply both directions)]** オプションを無効にした場合は、他のフィルタチェーンに対してこの手順を繰り返します。

- b) 開いた **[フィルタ チェーンの追加]** ウィンドウで、**[名前 (Name)]** ドロップダウンメニューから前の手順で追加したフィルタを選択します。
- c) **[保存 (Save)]** をクリックして、フィルタをコントラクトに追加します。

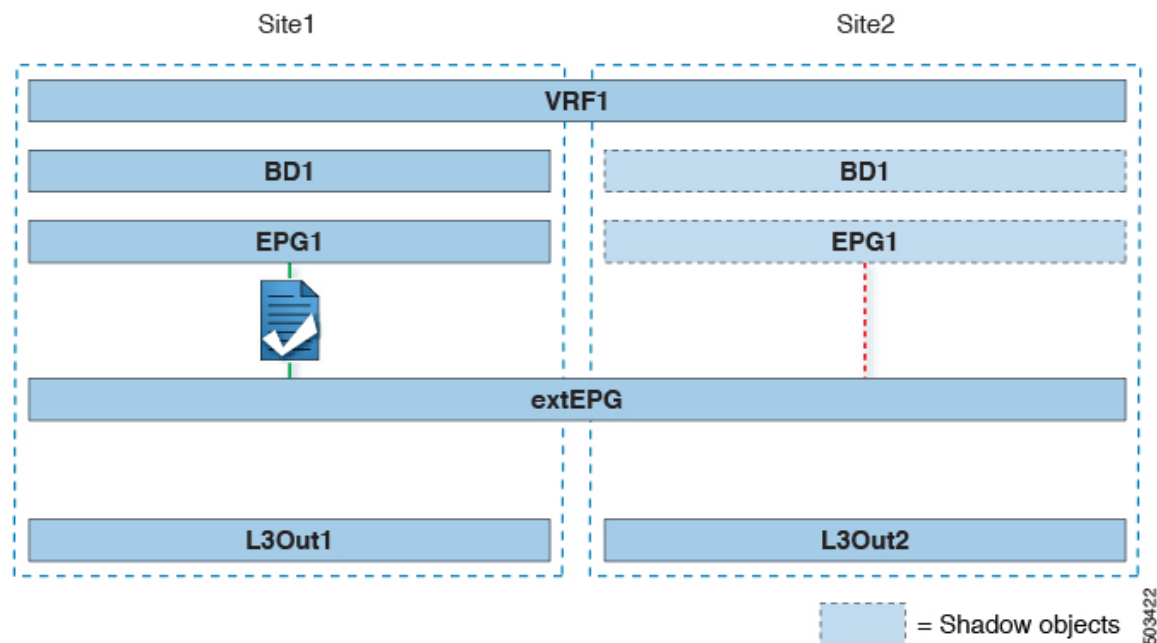
使用例

アプリケーション EPG のサイト間 L3Out (VRF内)

ここでは、アプリケーション EPG の一部であるエンドポイントが、同じ VRF (intra-VRF) 内にある別のサイトに展開された L3Out を介して到達可能な外部ネットワークドメインと通信できるようにするために必要な設定について説明します。

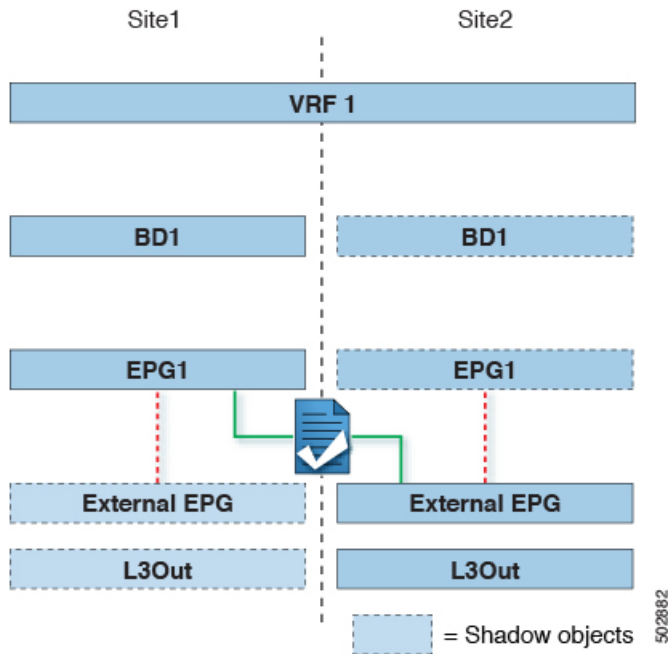
最初の図は、拡大された外部 EPG と、両方のサイトで作成される関連づけられた L3Out を示しています。アプリケーション EPG (EPG1) はサイト 1 で作成され、外部 EPG とのコントラクトがあります。この使用例は、別のサイトの L3Out が外部リソースの共通セットへのアクセスを提供する場合に推奨されます。ポリシー定義と外部トラフィック分類が簡素化され、独立した APIC ドメインの各 L3Out に個別にルートマップポリシーを適用できます。

図 19: 拡張された外部 EPG



次の 2 番目の図は、同様の使用例を示していますが、外部 EPG は物理 L3Out が配置されているサイトだけに導入されています。アプリケーション EPG とコントラクトは、1 つのサイトの EPG と他方の物理 L3Out 間のトラフィックフローを可能にするのと全く同じ方法で設定します。

図 20: 拡張されていない (サイトローカル) の外部 EPG



次の手順では、最も一般的なシナリオである図1に示す使用例を実装するために必要な設定について説明します。図2に示すユースケースを導入する場合は、若干の変更を加えて手順を調整できます。

始める前に

次のものがすでに設定されている必要があります。

- 3つのテンプレートを持つスキーマ。

アプリケーションEPGやL3Outsなど、そのサイトに固有のオブジェクトを設定する各サイトのテンプレート (template-site1 や template-site2 など) を作成します。さらに、ストレッチされたオブジェクト (この場合は外部 EPG) に使用する別のテンプレート (template-stretched など) を作成します。

- [サイト間L3OutおよびVRFの作成またはインポート \(218ページ\)](#) セクションで説明されている各サイトのL3Outs。

この使用例では、各サイト固有のテンプレートに個別のL3Outがインポートまたは作成されます。

- [サイト間L3Outを使用するための外部EPGの設定 \(221ページ\)](#) で説明されているように、サイト間L3Outの外部EPG。

この使用例では、外部EPGは、ストレッチされたテンプレート (template-stretched) で定義されたストレッチされたオブジェクトとして設定されます。外部EPGが外部アドレス空間全体へのアクセスを提供すると仮定すると、より具体的なプレフィックスの長いリストを指定しないように、0.0.0.0/0プレフィックスを分類用に設定することを推奨します。

- [サイト間 L3Out のコントラクトの作成 \(224 ページ\)](#) で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。
ストレッチテンプレート (template-stretched) でコントラクトとフィルタを作成することをお勧めします。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 アプリケーション EPG とブリッジ ドメインのスキーマとテンプレートを選択します。

この使用例では、テンプレートを Site1 に関連付けます。

ステップ 4 L3Out とは別の VRF に属するアプリケーション EPG とそのブリッジ ドメインを設定します。

サイト間 L3Out を使用する EPG がすでにある場合は、この手順をスキップできます。

通常のように、EPG およびブリッジ ドメインを新規に作成するか、既存のものをインポートします。

ステップ 5 アプリケーション EPG にコントラクトを割り当てます。

- EPG を選択します。
- 右側のサイドバーで、[+コントラクト (+Contract)] をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG がコンシューマかプロバイダかを選択できます。

ステップ 6 コントラクトを、リモート L3Out にマップされた外部 EPG に割り当てます。

- 外部 EPG が配置されている template-stretched を選択します。
- 外部 EPG を選択します。
- 右側のサイドバーで、[+コントラクト (+Contract)] をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG をコンシューマとして選択した場合は、外部 EPG のプロバイダを選択します。それ以外の場合は、外部 EPG のコンシューマを選択します。

ステップ 7 アプリケーション EPG のブリッジ ドメインを L3Out に関連付けます。

これにより、BD サブネットを L3Out から外部ネットワーク ドメインにアドバタイズできます。BD に関連付けられたサブネットは、L3Out からアドバタイズされるように [外部アドバタイズ (Advertised Externally)] オプションを使用して設定する必要があります。

- 左側のサイドバーの [サイト (Sites)] の下で、アプリケーション EPG のテンプレートを選択します。
- アプリケーション EPG に関連付けられたブリッジ ドメインを選択します。
- 右側のサイドバーで、[+ L3Out] をクリックします。
- 作成したサイト間 L3Out を選択します。

図1に示す使用例では、BD を Site1 と Site2 で定義された両方の L3Out に関連付けて、外部ネットワークが両方のパスから EPG にアクセスできるようにします。特定のポリシーを L3Out または外部ルータ

に関連付けて、特定の L3Out パスが着信トラフィックに通常優先されるようにすることができます。リモートサイトの L3Out を介した最適ではないインバウンドトラフィックパスを回避するために、EPG と BD が (特定の例のように) サイトに対してローカルである場合、これを推奨します。

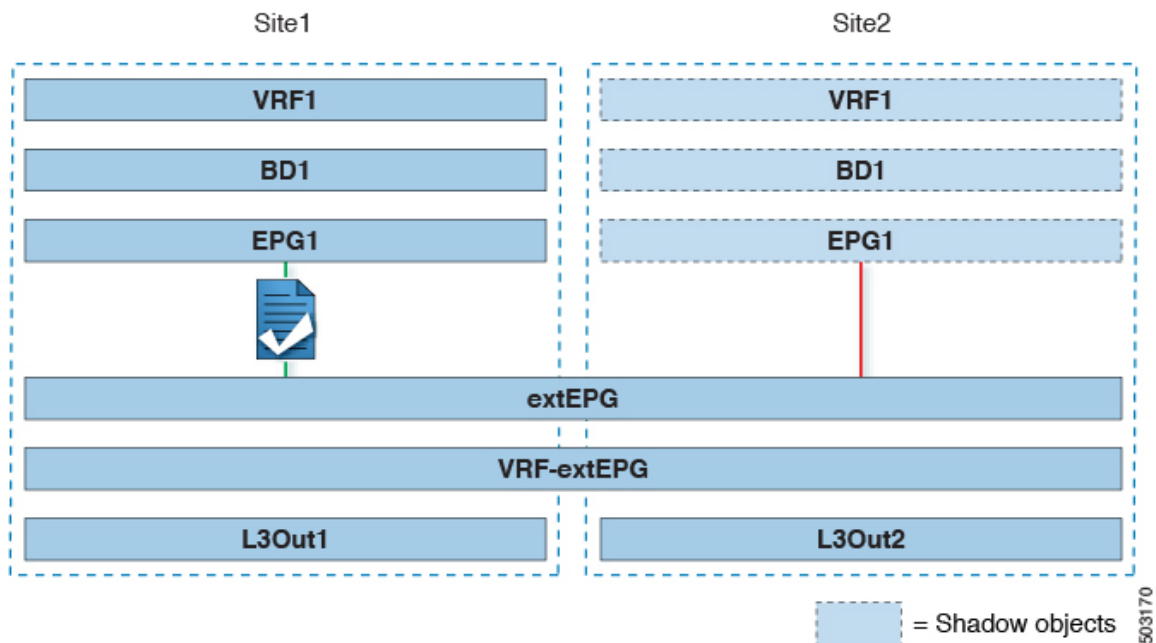
ステップ 8 スキーマを展開します。

アプリケーション EPG のサイト間 L3Out との共有サービス (Inter-VRF)

ここでは、1 つの VRF のアプリケーション EPG の一部であるエンドポイントが、別のサイトに展開された L3Out を介して到達可能な外部ネットワーク ドメインと通信できるようにするために必要な設定について説明します。これは「共有サービス」とも呼ばれます。

このシナリオは、別のサイトの L3Out が外部リソースの共通セットへのアクセスを提供する場合に推奨されます。ポリシー定義と外部トラフィック分類が簡素化され、独立した APIC ドメインの各 L3Out に個別にルートマップポリシーを適用できます。

図 21: ストレッチ外部 EPG、サイトローカル L3Out、およびアプリケーション EPG のいずれかになります。



次の手順では、図 3 に示す使用例を実装するために必要な設定について説明します。

始める前に

次のものがすでに設定されている必要があります。

- 3 つのテンプレートを持つスキーマ。

アプリケーション EPG や L3Outs など、そのサイトに固有のオブジェクトを設定するサイトごとのテンプレート (template-site1 や template-site2 など) を作成します。さらに、

ストレッチされたオブジェクト（この場合は外部 EPG）に使用する別のテンプレート（`template-stretched` など）を作成します。

- **サイト間 L3Out および VRF の作成またはインポート (218 ページ)** セクションで説明されている各サイトの L3Outs。

この使用例では、各サイト固有のテンプレートに個別の L3Out がインポートまたは作成されます。

- **サイト間 L3Out を使用するための外部 EPG の設定 (221 ページ)** で説明されているように、サイト間 L3Out の外部 EPG。

この使用例では、外部 EPG は、ストレッチされたテンプレート（`template-stretched`）で定義されたストレッチされたオブジェクトとして設定されます。外部 EPG が外部アドレス空間全体へのアクセスを提供すると仮定すると、より具体的なプレフィックスの長いリストを指定しないように、`0.0.0.0/0` プレフィックスを分類用に設定することを推奨します。

この特定の共有サービスの使用例では、リモート L3Out の外部 EPG に関連付けられたサブネットの**共有ルート制御フラグ**と**共有セキュリティインポートフラグ**を有効にする必要があります。外部 EPG の分類に `0.0.0.0/0` プレフィックスを使用している場合は、**共有ルート制御フラグ**に加えて、**集約共有ルートフラグ**も有効にします。

- **サイト間 L3Out のコントラクトの作成 (224 ページ)** で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。

ストレッチテンプレート（`template-stretched`）でコントラクトとフィルタを作成することをお勧めします。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、**[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)]** を選択します。

ステップ 3 アプリケーション EPG とブリッジドメインのスキーマとテンプレートを選択します。

この使用例では、テンプレートを Site1 に関連付けます。

ステップ 4 L3Out とは別の VRF に属するアプリケーション EPG とそのブリッジドメインを設定します。

サイト間 L3Out を使用する EPG がすでにある場合は、この手順をスキップできます。

通常のように、EPG およびブリッジドメインを新規に作成するか、既存のものをインポートします。

ステップ 5 アプリケーション EPG にコントラクトを割り当てます。

- EPG を選択します。
- 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG がコンシューマかプロバイダかを選択できます。

- (注) アプリケーション EPG をプロバイダとして設定する場合は、そのルートを L3Out VRF にリークするために、EPG の下でも BD ですでに定義されているサブネットを設定する必要があります。サブネットの BD で使用されるのと同じフラグも EPG で設定する必要があります。さらに、EPG の下のサブネットでは、デフォルト ゲートウェイ機能が BD レベルで有効になっているため、**[デフォルト SVI ゲートウェイなし (No default SVI Gateway)]** フラグも有効にする必要があります。

ステップ 6 コントラクトを、L3Out にマップされた外部 EPG に割り当てます。

- 外部 EPG が配置されている `template-stretched` を選択します。
- 外部 EPG を選択します。
- 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG をコンシューマとして選択した場合は、外部 EPG のプロバイダを選択します。それ以外の場合は、外部 EPG のコンシューマを選択します。

ステップ 7 アプリケーション EPG のブリッジ ドメインを L3Out に関連付けます。

これにより、BD サブネットを L3Out から外部ネットワーク ドメインにアダプタイズできます。BD に関連付けられたサブネットは、L3Out からアダプタイズされるように **[外部アダプタイズ (Advertised Externally)]** オプションを使用して設定する必要があります。

- 左側のサイドバーの **[サイト (Sites)]** の下で、アプリケーション EPG のテンプレートを選択します。
- アプリケーション EPG に関連付けられたブリッジ ドメインを選択します。
- 右側のサイドバーで、**[+ L3Out]** をクリックします。
- 作成したサイト間 L3Out を選択します。

図1に示す使用例では、BD を Site1 と Site2 で定義された両方の L3Out に関連付けて、外部ネットワークが両方のパスから EPG にアクセスできるようにします。特定のポリシーを L3Out または外部ルータに関連付けて、特定の L3Out パスが着信トラフィックに通常優先されるようにすることができます。リモートサイトの L3Out を介した最適ではないインバウンドトラフィック パスを回避するために、EPG と BD が（特定の例のように）サイトに対してローカルである場合、これを推奨します。

ステップ 8 スキーマを展開します。

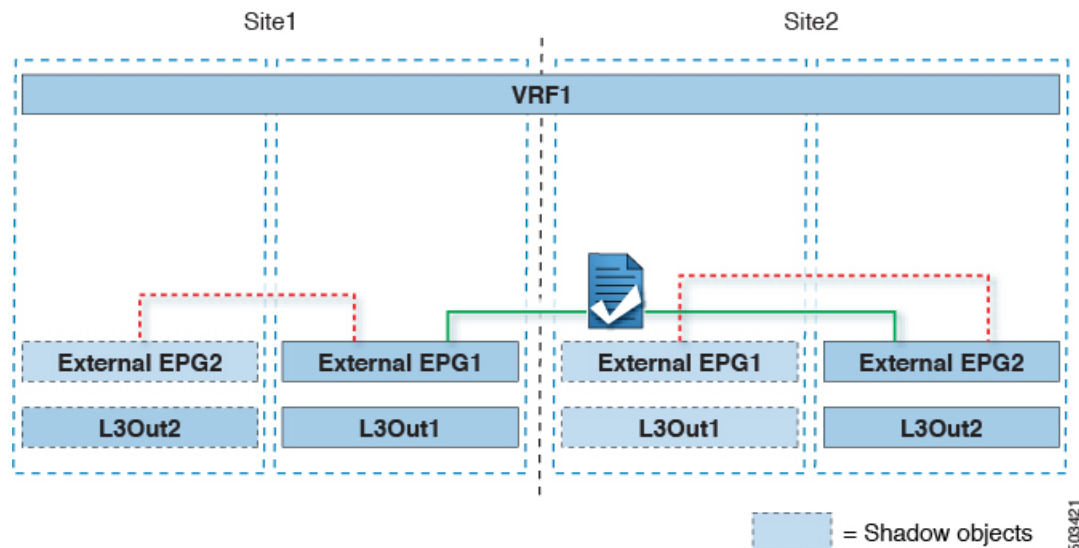
サイト間中継ルーティング

このセクションでは、マルチサイトドメインが分散ルータとして機能し、異なるサイトに展開された L3Out の背後に接続されているエンティティ（エンドポイント、ネットワーク デバイス、サービス ノードなど）間の通信を可能にする使用例について説明します。この機能は通常、サイト間中継ルーティングと呼ばれます。サイト間中継ルーティングは、VRF 内および VRF 間のユースケースでサポートされます。

次の図は、異なるサイトに設定されている2つの L3Outs (l3out1 と l3out2) を示しています。各 L3Out はそれぞれの外部 EPG (ExtEPG1 および ExtEPG2) に関連付けられています。2つの外部

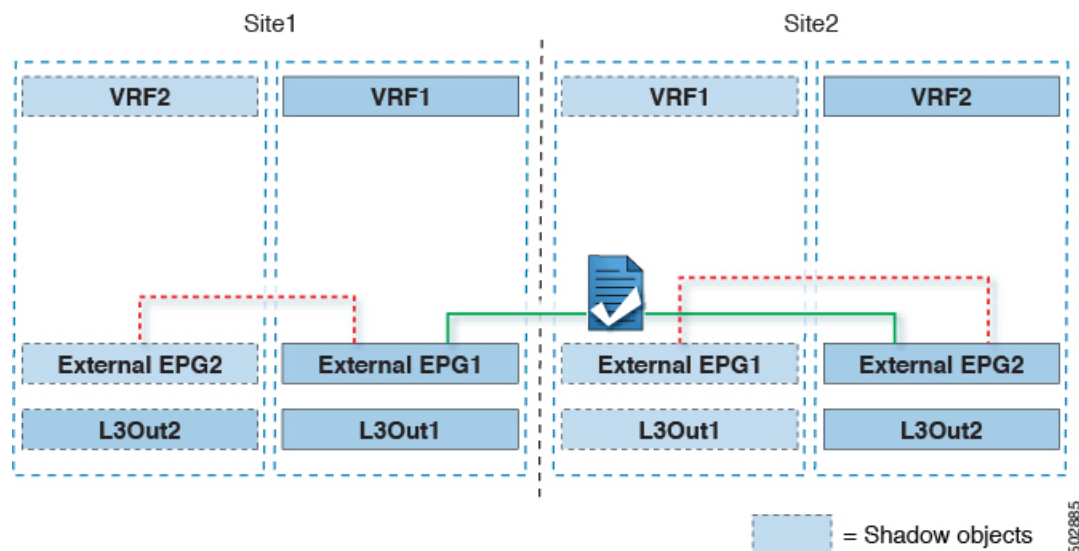
EPG 間のコントラクトにより、2つの異なるサイトの2つの異なる L3Outs の背後にあるエンドポイント間の通信が可能になります。

図 22: VRF サイト内中継ルーティング



各サイトの L3Out が異なる VRF にある場合も、同様の設定を使用できます。

図 23: VRF サイト間中継ルーティング



図では、外部 EPG と、関連付けられた L3Out がサイトローカルオブジェクトとして展開される、2つのシナリオを示しています。サイト間中継ルーティングは、サイト間で EPG がストレッチされていない場合、一方がストレッチされている場合、両方がストレッチされている場合という、すべての組み合わせをサポートしています。

サイト間中継ルーティングを導入する場合、サイト間で定義された異なる外部 EPG が異なる外部アドレス空間へのアクセスを提供する（明らかに重複しない）ことが前提となります。したがって、分類に使用されるプレフィックスの設定には、いくつかのオプションがあります。

- 両方の外部 EPG で同じ 0.0.0.0/0 プレフィックスを定義して、L3Out1 の境界リーフ ノードで受信した着信トラフィックが Ext-EPG1 にマッピングされ、L3Out2 で受信した着信トラフィックが Ext-EPG2 にマッピングされるようにします。L3Out は別のファブリックで定義されているため、この設定で競合の問題は発生しません。

L3Out1 で受信した外部プレフィックスは、L3Out2 からアドバタイズする必要があります。その逆も同様です。両方の外部 EPG で 0.0.0.0/0 を分類サブネットとして使用している場合は、**[エクスポート ルート制御 (Export Route Control)]** および **[集約エクスポート (Aggregate Export)]** フラグを有効にするだけで十分です。

- 外部 EPG ごとに特定のプレフィックスを定義します。この場合、ローカル外部 EPG とリモート外部 EPG 間のコントラクトのためにシャドウ外部 EPG がそのサイトで作成されるたびに、サイトの APIC によって障害が発生するのを回避するために、プレフィックスが重複していないことを確認する必要があります。

特定のプレフィックスを使用する場合は、外部 EPG1 で分類用に設定したのと同じプレフィックスを、**[エクスポート ルート制御 (Export Route Control)]** フラグを立てて、外部 EPG2 で設定する必要があります。逆の場合も同じです。



- (注) 2つの分類アプローチのどちらを導入する場合でも、VRF 間シナリオでは、**[共有ルート制御 (Shared Route Control)]**（加えて **[集約共有ルート (Aggregate Shared Routes)]** も 0.0.0.0/0 を使用する場合には必要）および **[共有セキュリティ インポート (Shared Security Import)]** の各フラグを設定する必要があります。

始める前に

次のものがすでに設定されている必要があります。

- 3つのテンプレートを持つスキーマ。

アプリケーション EPG や L3Outs など、そのサイトに固有のオブジェクトを設定するサイトごとのテンプレート (template-site1 や template-site2 など) を作成します。さらに、ストレッチされたオブジェクト (この場合は外部 EPG) に使用する別のテンプレート (template-stretched など) を作成します。

- [サイト間 L3Out および VRF の作成またはインポート \(218 ページ\)](#) セクションで説明されている各サイトの L3Outs。

この使用例では、各サイト固有のテンプレートに個別の L3Out がインポートまたは作成されます。

- 異なるサイトにある2つの異なる L3Outs 用の2つの異なる外部 EPG。 [サイト間 L3Out を使用するための外部 EPG の設定 \(221 ページ\)](#) の説明に従って、同じ手順を使用して両方の外部 EPG を作成できます。

- [サイト間L3Outのコントラクトの作成 \(224ページ\)](#) で説明されているように、サイトごとに定義された L3Out 外部 EPG の間でコントラクトを使用します。
ストレッチテンプレート (template-stretched) でコントラクトとフィルタを作成することをお勧めします。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 いずれかの外部 EPG にコントラクトを割り当てます。

- 外部 EPG が配置されているスキーマとテンプレートを選択します。
- 外部 EPG を選択します。
- 右側のサイドバーで、[+コントラクト (+Contract)] をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

コンシューマまたはプロバイダを選択します。

ステップ 4 他の外部 EPG にコントラクトを割り当てます。

- 外部 EPG が配置されているスキーマとテンプレートを選択します。
- 外部 EPG が配置されているテンプレートを参照します。
- 外部 EPG を選択します。
- 右側のサイドバーで、[+コントラクト (+Contract)] をクリックします。
- 前のセクションで作成したコントラクトとそのタイプを選択します。

プロバイダまたはコンシューマを選択します。

ステップ 5 適切なサイトにテンプレートを展開します。



第 21 章

PBR を使用したサイト間 L3Out

- [PBR を使用したサイト間 L3Out \(237 ページ\)](#)
- [サポートされる使用例 \(238 ページ\)](#)
- [注意事項と制約事項 \(242 ページ\)](#)
- [APIC サイトの設定 \(243 ページ\)](#)
- [テンプレートの作成 \(248 ページ\)](#)
- [サービス グラフの設定 \(249 ページ\)](#)
- [コントラクトのフィルタの作成 \(251 ページ\)](#)
- [アプリケーション EPG の作成 \(257 ページ\)](#)
- [L3Out 外部 EPG の作成 \(260 ページ\)](#)

PBR を使用したサイト間 L3Out

Cisco Application Centric Infrastructure (ACI) ポリシーベースリダイレクト (PBR) は、ファイアウォールやロードバランサなどのサービスアプライアンス、および侵入防御システム (IPS) のトラフィックリダイレクションを可能にします。一般的な使用例としては、プールしてアプリケーションプロファイルに合わせて調整すること、また容易にスケールアップすることができ、サービス停止の問題が少ないサービスアプライアンスのプロビジョニングがあります。PBR により、コンシューマとプロバイダエンドポイントの間のコントラクトに基づくサービスアプライアンスの挿入は簡素化されます。このことは、それらすべてが同じ仮想ルーティングおよびフォワーディング (VRF) インスタンスに存在する場合でも成り立ちます。

PBR の展開には、ルートリダイレクトポリシーおよびクラスタのリダイレクトポリシーの設定と、これらのポリシーを使用するサービスグラフテンプレートの作成が含まれます。サービスグラフテンプレートを展開した後、EPG 間のコントラクトにアタッチして、そのコントラクトに従うすべてのトラフィックが、作成した PBR ポリシーに基づいてサービスグラフデバイスにリダイレクトされるようにすることができます。これにより、同じ 2 つの EPG 間のどのタイプのトラフィックを L4-L7 デバイスにリダイレクトし、どのタイプのトラフィックを直接許可するかを選択できます。

サービスグラフおよび PBR に固有の詳細情報については、『[Cisco APIC Layer 4 to Layer 7 Services Deployment Guide](#)』を参照してください。

マルチサイト展開での PBR のサポート

Cisco Multi-Site は以前より、Cisco APIC リリース 3.2(1) 以降、PBR との EPG 間 (East-West) および L3Out-to-EPG (North-South) コントラクトをサポートしています。ただし、サイト間の L3Out-to-EPG (site1 の外部エンドポイントから site2 のエンドポイントへのトラフィック) のケースは、両方のサイトにローカル L3Out がある場合にのみサポートされていました。サイト間 L3Out の使用例は、[サイト内 L3Out \(215 ページ\)](#) の章で説明した例と設定に限定されていました。同様に、PBR とのサービスグラフ統合はありますが、サイト間 L3Out はありません。詳細については、『[Cisco Multi-Site and Service Node Integration White Paper](#)』を参照してください。

Cisco APIC リリース 4.2(5) 以降では、サイトを越えて PBR を使用する L3Out-to-EPG (サイト間 L3Out) の使用例が拡張され、アプリケーション EPG にローカル L3Out がない場合や、ローカル L3Out がダウンしている場合に対応できるようになりました。

サポートされる使用例

次の図は、アプリケーション EPG の ACI 内部エンドポイントと、サポートされているサイト間 L3Out with PBR 使用例の別のサイトの L3Out を経由する外部エンドポイント間のトラフィックフローを示しています。

これらの例を設定するワークフローは同じですが、オブジェクトを同じ VRF で作成するか、異なる VRF で作成するか (VRF 間と VRF 内)、およびオブジェクトを展開する場所 (ストレッチか非ストレッチか) のみが異なります。

1. [L4-L7 デバイスおよび PBR ポリシーの作成と設定 \(244 ページ\)](#) の説明に従って、サイトの APIC で L4-L7 デバイスを直接作成します。

Nexus Dashboard Orchestrator からデバイスと PBR ポリシーを作成することはできないため、これらのオプションを設定するには、各サイトの APIC に直接ログインする必要があります。

2. [テンプレートの作成 \(248 ページ\)](#) の説明に従って、必要なテンプレートを作成します。
すべてのサイトに展開されたすべてのオブジェクトを含む単一の拡張テンプレートを作成することをお勧めします。次に、各サイト専用のオブジェクトを含む各サイトの追加テンプレート。
3. [サービスグラフの設定 \(249 ページ\)](#) の説明に従って、サービスグラフを作成して設定します。
4. [コントラクトのフィルタの作成 \(251 ページ\)](#) の説明に従って、アプリケーション EPG と別のサイトの L3Out を含む外部 EPG 間のすべてのトラフィックに使用するコントラクトとフィルタを作成します。
5. [アプリケーションプロファイルと EPG の作成 \(258 ページ\)](#) の説明に従って、VRF とリッジドメインを使用してアプリケーション EPG を作成します。

アプリケーション EPG を拡張するかどうかに応じて、これらのオブジェクトを異なるテンプレートで作成します。同様に、アプリケーション EPG と L3Out に同じ VRF または異なる VRF を使用することもできます。

6. [サイト間 L3Out および VRF の作成またはインポート \(260 ページ\)](#) の説明に従って、L3Out を作成します。
7. [サイト間 L3Out を使用するための外部 EPG の設定 \(221 ページ\)](#) の説明に従って、L3Out の外部 EPG を作成します。

Inter-VRF と Intra-VRF

アプリケーション EPG と外部 EPG を作成および設定する場合、アプリケーション EPG のブリッジドメインと L3Out に VRF を提供する必要があります。同じ VRF (intra-VRF) を使用するか、異なる VRF (inter-VRF) を使用するかを選択できます。

EPG 間のコントラクトを確立する場合は、1 つの EPG をプロバイダとして指定し、もう 1 つの EPG をコンシューマとして指定する必要があります。

- 両方の EPG が同じ VRF にある場合、どちらか一方がコンシューマまたはプロバイダになることができます。
- EPG が異なる VRF にある場合は、外部 EPG がプロバイダーであり、アプリケーション EPG がコンシューマである必要があります。

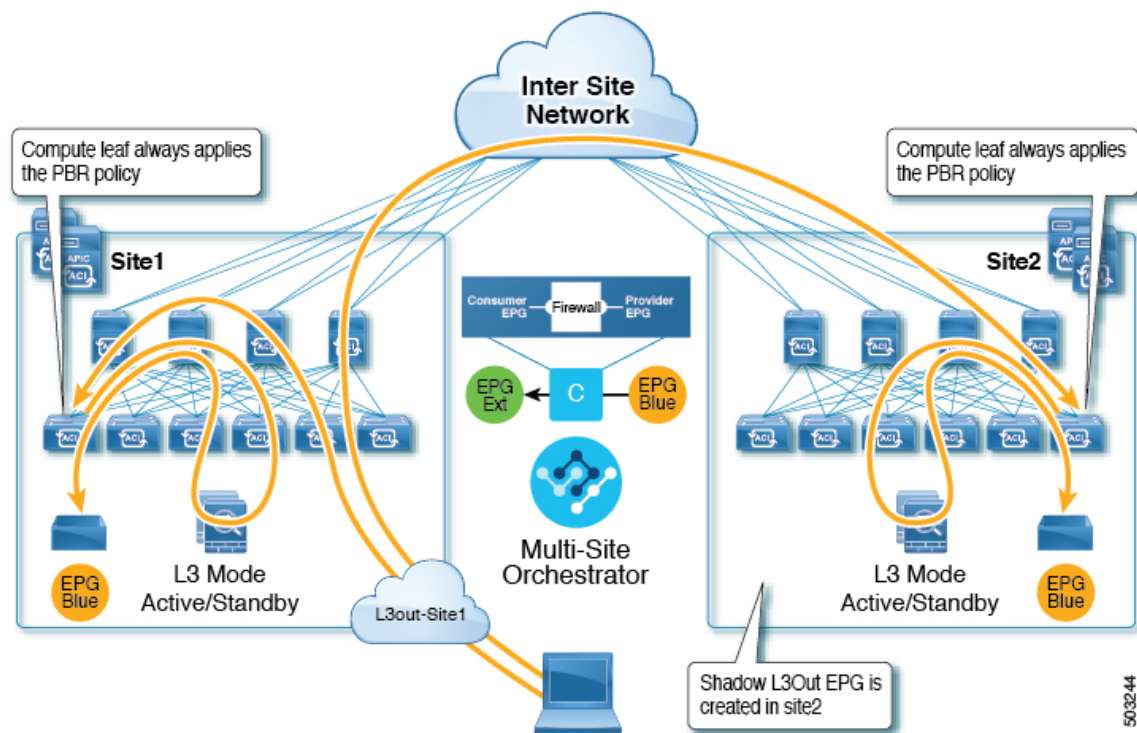
拡張された EPG

この使用例は、2 つのサイト間で拡張される単一のアプリケーション EPG と、1 つのサイトでのみ作成される単一の L3Out を示しています。アプリケーション EPG のエンドポイントが L3Out と同じサイトにあるか、他のサイトにあるかに関係なく、トラフィックは同じ L3Out を通過します。ただし、トラフィックは常にエンドポイントのサイトに対してローカルなサービスノードを通過します。



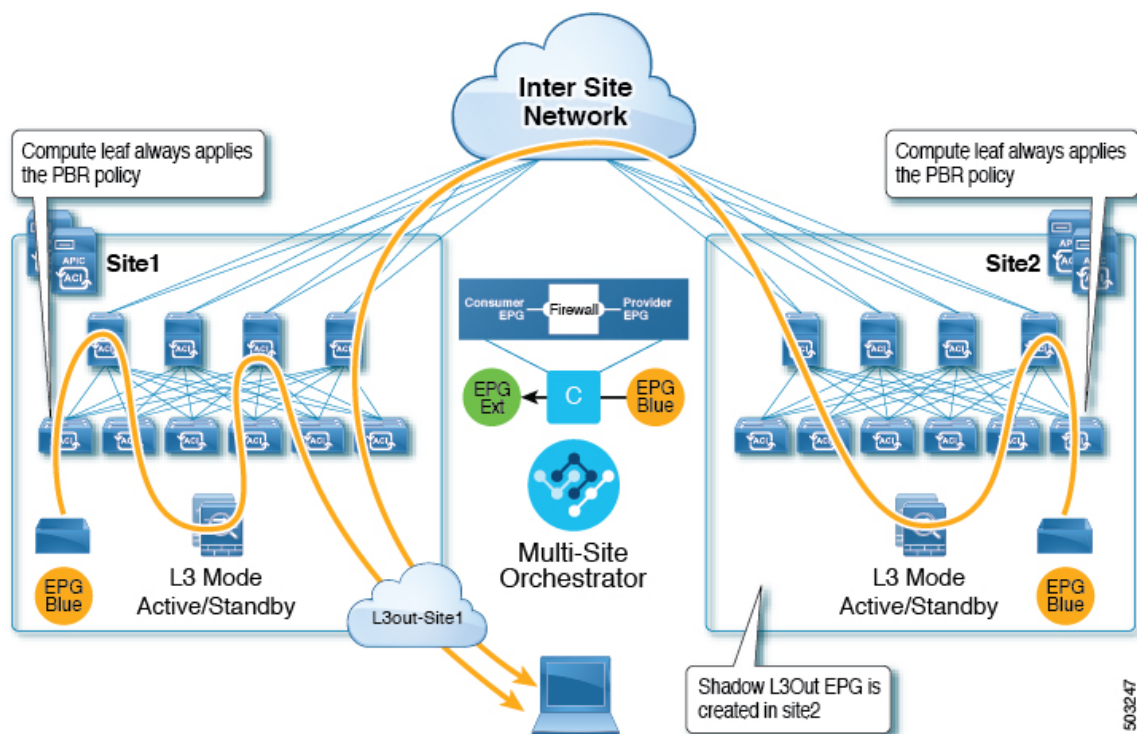
-
- (注) 外部 EPG が拡張され、各サイトに独自の L3Out があるが、トラフィックの発信元または宛先であるサイトの L3Out がダウンしている場合も、同じフローが適用されます。
-

図 24: インバウンドトラフィック



503244

図 25: アウトバウンドトラフィック



503247

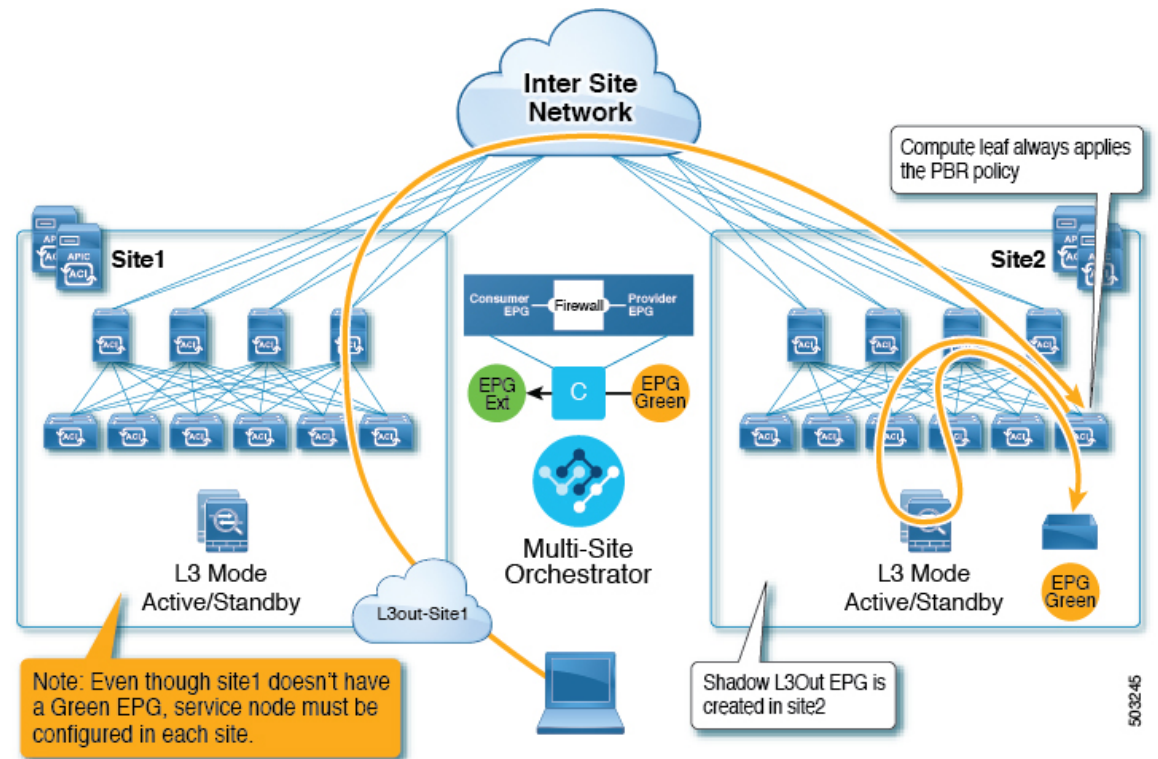
サイトローカル EPG

この使用例は、North-South トラフィックに他のサイトの L3Out を使用するサイトローカルアプリケーション EPG を示しています。前の例と同様に、すべてのトラフィックは EPG のサイトローカルサービス グラフ デバイスを使用します。



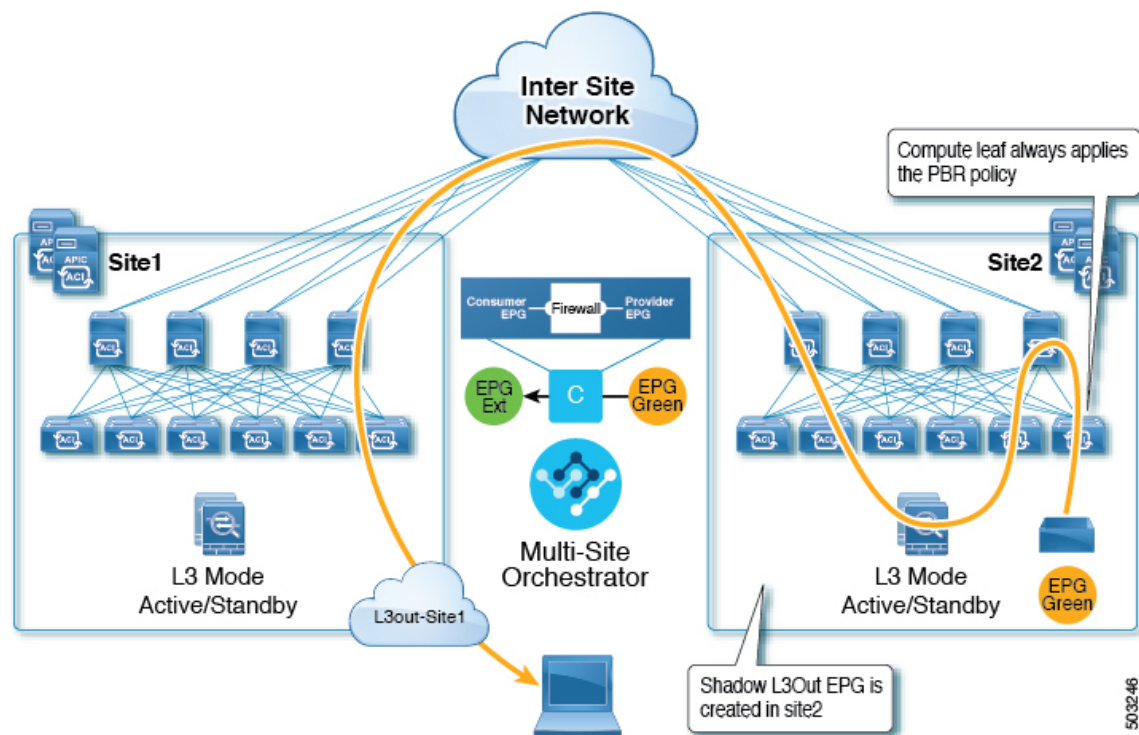
- (注) 外部 EPG が拡張され、各サイトに独自の L3Out があり、EPG のローカル L3Out がダウンしている場合も、同じフローが適用されます。

図 26: インバウンドトラフィック



503245

図 27: アウトバウンドトラフィック



503246

注意事項と制約事項

サイト間 L3Out を設定する際には次の制約事項が適用されます。

- PBR を使用しないサイト間 L3Out の使用例については、[サイト内 L3Out \(215 ページ\)](#) を参照してください。
- PBR を使用したサイト間 L3Out では、次の使用例がサポートされています。
 - アプリケーション EPG をコンシューマとする Inter-VRF サイト間 L3Out。
VRF 間コントラクトの場合、L3Out がプロバイダである必要があります。
 - アプリケーション EPG がプロバイダまたはコンシューマのいずれかである VRF 内サイト間 L3Out
 - PBR を使用したサイト間中継ルーティング (L3Out-to-L3Out) はサポートされていません。
- 上記の使用例は、Cisco APIC リリース 4.2(5) またはリリース 5.1(x) を実行しているサイトでサポートされています。Cisco APIC リリース 5.0(x) を実行しているサイトではサポートされません。

- サポートされるすべてのケースで、アプリケーション EPG をストレッチすることも、ストレッチしないこともできます。
- サービス グラフ デバイスは、サイト間 L3Out 外部 EPG と PBR コントラクトを持つアプリケーション EPG を持たないサイトを含め、各サイトで定義する必要があります。
- ワンアーム展開モデルとツーアーム展開モデルの両方がサポートされています。
ワンアーム展開では、サービスグラフの内部インターフェイスと外部インターフェイスの両方が同じブリッジドメインに接続されます。ツーアーム展開では、サービス グラフ インターフェイスは個別の BD に接続されます。
- PBR を使用してロード バランサを設定する場合、ロード バランサと仮想 IP (VIP) の実サーバは同じサイトに存在する必要があります。PBR がディセーブルの場合、ロード バランサと実サーバは異なるサイトに存在できます。
- PBR を設定する場合、宛先は L1、L2、または L3 です。

APIC サイトの設定

外部 TEP プールの設定

サイト間 L3Out には、各ポッドの境界リーフ スイッチに外部 TEP アドレスが必要です。外部 TEP プールがすでに設定されている場合(たとえば、リモートリーフなどの別の機能のために)は、同じプールを使用できます。既存の TEP プールは Nexus Dashboard Orchestrator に継承され、インフラストラクチャ設定の一部として GUI に表示されます。それ以外の場合は、この項で説明されているように、GUI で TEP プールを追加できます。



(注) すべてのポッドに一意の TEP プールを割り当てる必要があり、ファブリック内の他の TEP プールと重複しないようにする必要があります。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。
- ステップ 3 メイン ペインの右上にある [構成 (Configure)] をクリックします。
- ステップ 4 左側のサイドバーで、設定するサイトを選択します。
- ステップ 5 メイン ウィンドウで、サイト内のポッドをクリックします。
- ステップ 6 右側のサイドバーで、[+ TEP プールを追加 (+Add TEP Pool)] をクリックします。
- ステップ 7 [TEP プールの追加 (Add TEP pool)] ウィンドウで、そのサイトに対して設定する外部 TEP プールを指定します。

(注) 追加しようとしている TEP プールが他の TEP プールまたはファブリックアドレスと重複していないことを確認する必要があります。

ステップ 8 このプロセスを、サイト間の L3Outs を使用する予定のサイトおよびポッドごとに繰り返します。

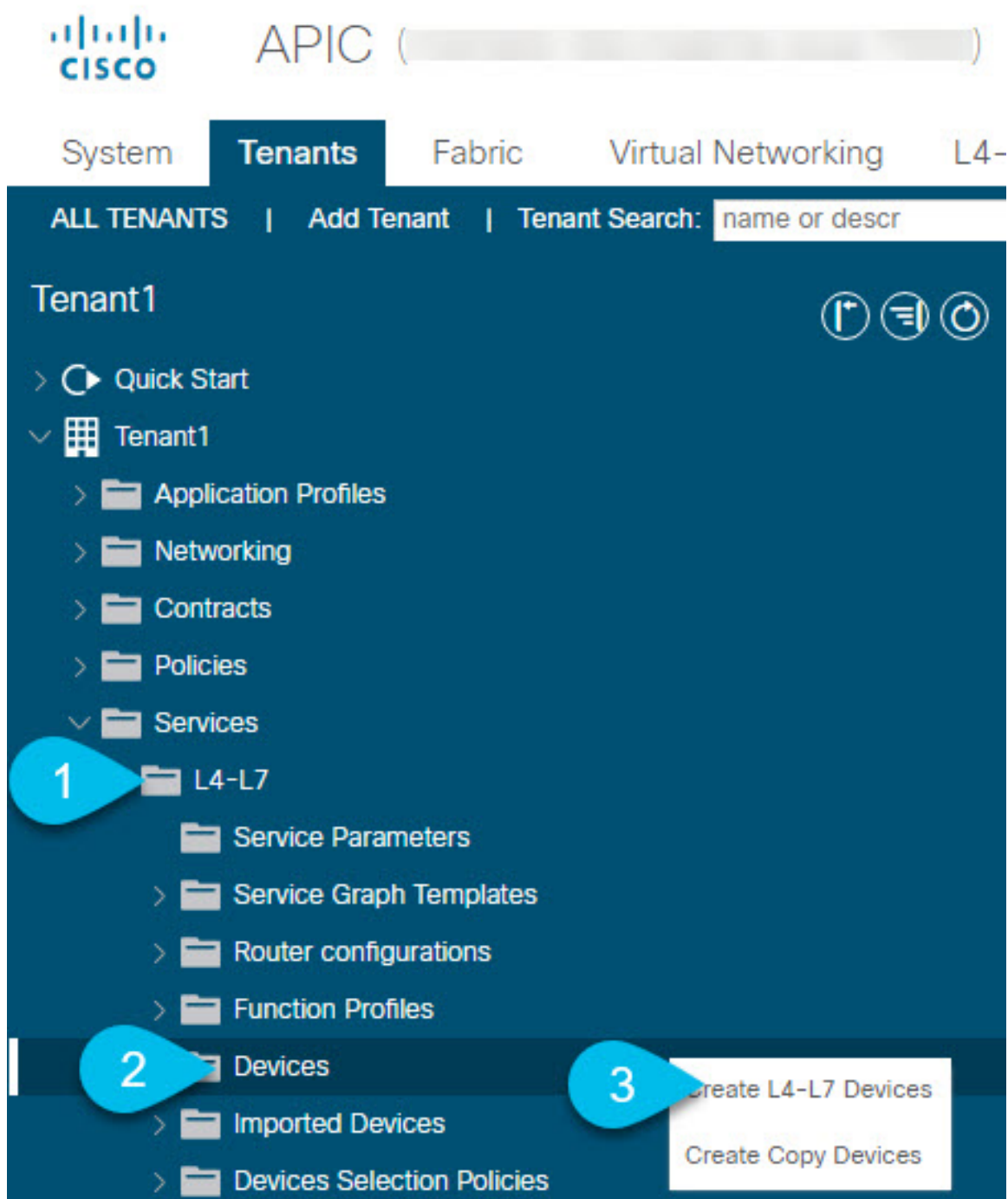
L4-L7 デバイスおよび PBR ポリシーの作成と設定

サービス グラフ デバイスを作成し、各サイトの APIC で PBR ポリシーを直接定義する必要があります。

ステップ 1 Cisco APIC にログインします。

ステップ 2 上部のメニューバーで **[テナント (Tenants)]** をクリックし、デバイスを作成するテナントを選択します。

ステップ 3 L4-L7 デバイスを作成します。



- 左側のサイドバーで、<tenant-name>> [サービス (Services)]> [L4-L7] カテゴリを展開します。
- [デバイス (Devices)] カテゴリを右クリックします。
- [L4-L7 デバイスの作成 (Create L4-L7 Devices)] を選択します。

[L4-L7 デバイスの作成 (Create L4-L7 Devices)] の設定ダイアログが開きます。

ステップ 4 L4-L7 デバイスを設定します。

次の図は、デバイスの設定サンプルを示しています。構成設定は、デバイスのタイプと目的によって異なります。

Create L4-L7 Devices

STEP 1 > General

1. General

General

Managed:

Name: Site1-FW

Service Type: Firewall

Device Type: CLOUD PHYSICAL **VIRTUAL**

VMM Domain: S1-VMM

Trunking Port:

VM Instantiation Policy: select an option

Promiscuous Mode:

Context Aware: Multiple **Single**

Function Type: GoThrough **GoTo**

Devices

The device mode can be single, HA or cluster. Create only one device for single, two for HA and at least 3 for cluster.

Name	VM Name	vCenter Name	Interfaces
ASAv1	MSO-SG-WP-ASAv1	vc1	g0/0 g0/1
ASAv2	MSO-SG-WP-ASAv2	vc1	g0/0 g0/1

Cluster

Cluster Interfaces:

Name	Concrete Interfaces
FW-external	ASAv1/g0/0,ASAv2/g0/0
FW-internal	ASAv1/g0/1,ASAv2/g0/1

Previous Cancel **Finish**

ステップ 5 PBR ポリシーを作成します。

- a) 左側のサイドバーで、<tenant-name>> [ポリシー(Policies)]> [プロトコル (Protocol)] カテゴリを展開します。
- b) [L4-L7 ポリシーベース リダイレクト (L4-L7 Policy-Based Redirect)] カテゴリを右クリックします。
- c) [L4-L7 ポリシーベース リダイレクトの作成 (Create L4-L7 Policy-Based Redirect)] を選択します。
[L4-L7 ポリシーベース リダイレクトの作成 (Create L4-L7 Policy-Based Redirect)] の設定ダイアログが開きます。

ステップ 6 PBR ポリシーを設定します。

次の図は、宛先 IP と MAC が追加されたサンプル PBR ポリシー設定を示しています。

構成設定は、作成するデバイスとポリシーのタイプと目的によって異なります。たとえば、PBR ポリシーでは、IP-SLA、ハッシュ アルゴリズム、レジリエント ハッシュなどの追加オプションを設定できます。

Create L4-L7 Policy-Based Redirect ? X

Name: 🔒

Description:

Destination Type: L1 L2 L3

IP SLA Monitoring Policy: ▼

Enable Pod ID Aware Redirection:

Hashing Algorithm: dip sip sip-dip-prototype

Enable Anycast:

Resilient Hashing Enabled:

L3 Destinations: 🗑️ +

IP	Destination Name	MAC	Redirect Health	IPv4/IPv6 Group	Description	Oper Status
192....		00:50:56:95:...				Ena...

Cancel
Submit

ステップ 7 他のサイトで必要なデバイスと PBR ポリシーを作成するには、前の手順を繰り返します。

テンプレートの作成

スキーマとテンプレートを作成する場合は、次の方法でテンプレートを分離することをお勧めします。

- すべてのサイト間で拡張されるすべてのオブジェクトを含む、単一の共有テンプレート。
- そのサイトにのみ展開するオブジェクトを含む、サイトごとに1つのテンプレート。

この例では、2つのサイトを使用するため、合計3つのテンプレートを作成します。各サイトに1つと、ストレッチされた1つです。

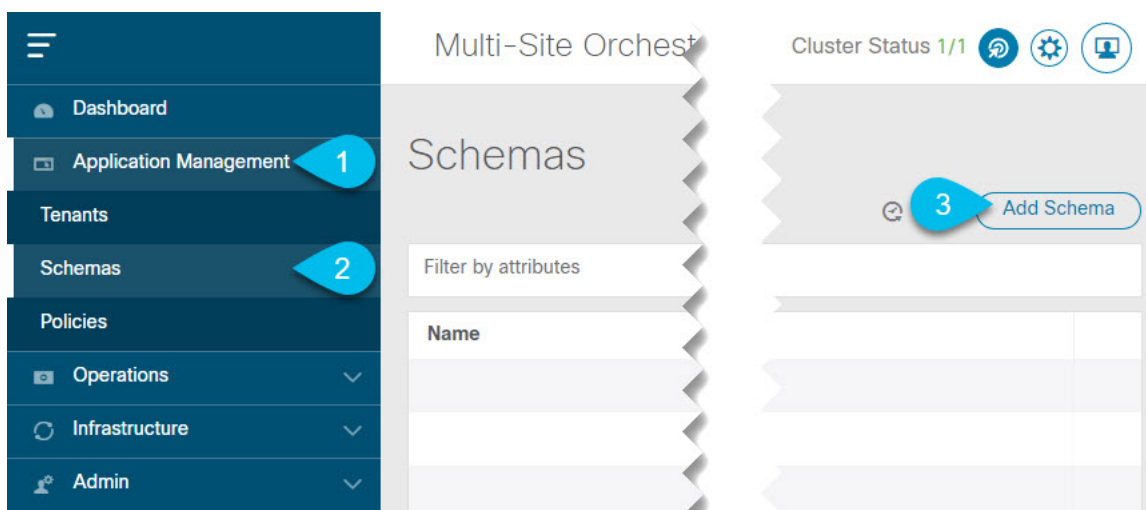
始める前に

次のものがが必要です。

- [注意事項と制約事項 \(242 ページ\)](#) を確認し、そこにリストされているすべての前提条件を完了していること。
- [外部 TEП プールの設定 \(218 ページ\)](#) および [L4-L7 デバイスおよび PBR ポリシーの作成と設定 \(244 ページ\)](#) の説明に従って、個々の APIC サイトの設定を完了していること。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

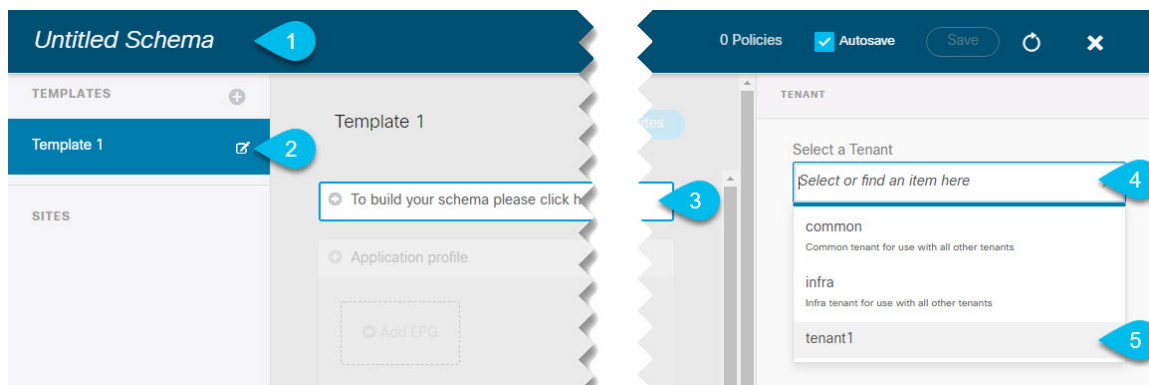
ステップ 2 スキーマを新規作成します。



- 左側のナビゲーションサイドバーで、[アプリケーション管理 (Application Management)] カテゴリを展開します。
- [スキーマ (Schemas)] を選択します。
- [スキーマの追加 (Add Schema)] をクリックして、新しいスキーマを作成します。

[スキーマの編集 (Edit Schema)] ウィンドウが開きます。

ステップ3 スキーマに名前を付け、テナントを選択します。



- [名称未設定のスキーマ (**Untitled Schema**)] をスキーマの名前に置き換えます。
[名称未設定のスキーマ (Untitled Schema)] の名前をクリックして編集します。
- テンプレートの名前を変更します。
左側のサイドバーで、テンプレートの上にマウスを移動し、[編集 (**Edit**)] アイコンをクリックします。
たとえば、`template-stretched`です。
- メイン ペインで、[スキーマを作成するエリアをクリックしてテナントを選択してください (**To build your schema please click here to select a tenant**)] をクリックします。
- 右側のサイドバーで、[テナントの選択 (**Select a Tenant**)] ドロップダウンをクリックします。
- テナントを選択します。

ステップ4 追加のテンプレートを作成します。

左側のサイドバーで、プラス (+) アイコン ([**テンプレート (Templates)**] の横にあるもの) をクリックして、サイト固有のテンプレートを追加します。次に、前述の手順と同じ手順に従ってテンプレートに名前を付け、テナントを選択します。

たとえば、`template-site1` と `template-site2` です。

サービス グラフの設定

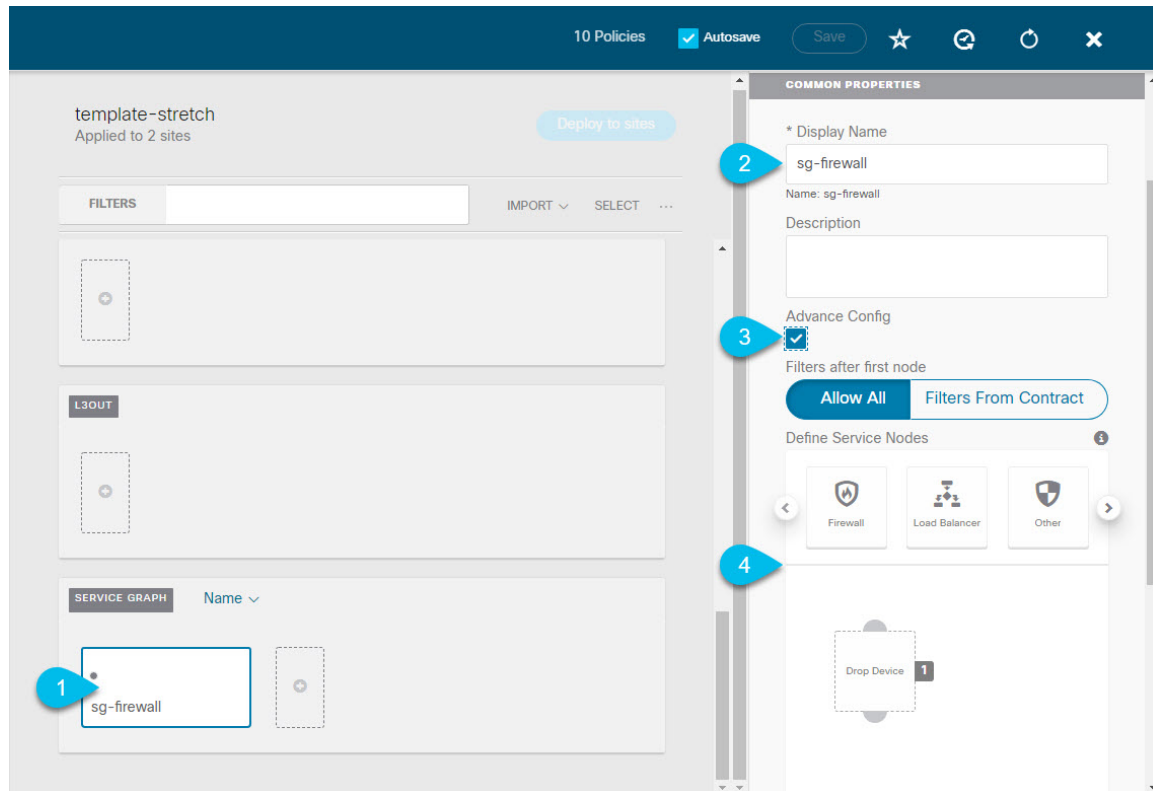
次のものがが必要です。

- [L4-L7 デバイスおよび PBR ポリシーの作成と設定 \(244 ページ\)](#) の説明に従い、サイトの APIC ごとに直接作成された L4-L7 デバイス。
- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

ここでは、サービスグラフの1つ以上のデバイスを設定する方法について説明します。

ステップ1 サービス グラフを作成するテンプレートを選択します。

template-stretchで単一のサービスグラフを作成しますが、この手順の後半で説明するように、サイトローカルデバイスを設定します。

ステップ2 サービス グラフを作成します。

- メインペインで、[サービス グラフ (Service Graph)] 領域までスクロールダウンして、[+] アイコンをクリックして新しいコントラクトを作成します。
- サービス グラフの [表示名 (Display Name)] を入力します。
- (オプション) [詳細設定 (Advanced Config)] オプションをオンにします。

このオプションでは、最初のサービス グラフ ノードの後にトラフィックを制限するかどうかを設定できます。このオプションを有効にしない場合、デフォルトでは、最初のサービス グラフ ノード以降のすべてのトラフィックが許可されます。

[詳細設定 (Advanced Config)] を有効にする場合は、次の2つのオプションのいずれかを選択します。

- [すべて許可 (Allow All)] : 契約サブジェクトの特定のフィルタの代わりにデフォルト (permit-all) フィルタを使用します。

これは、[詳細設定 (Advanced Config)] を無効にした場合と同じ動作です。

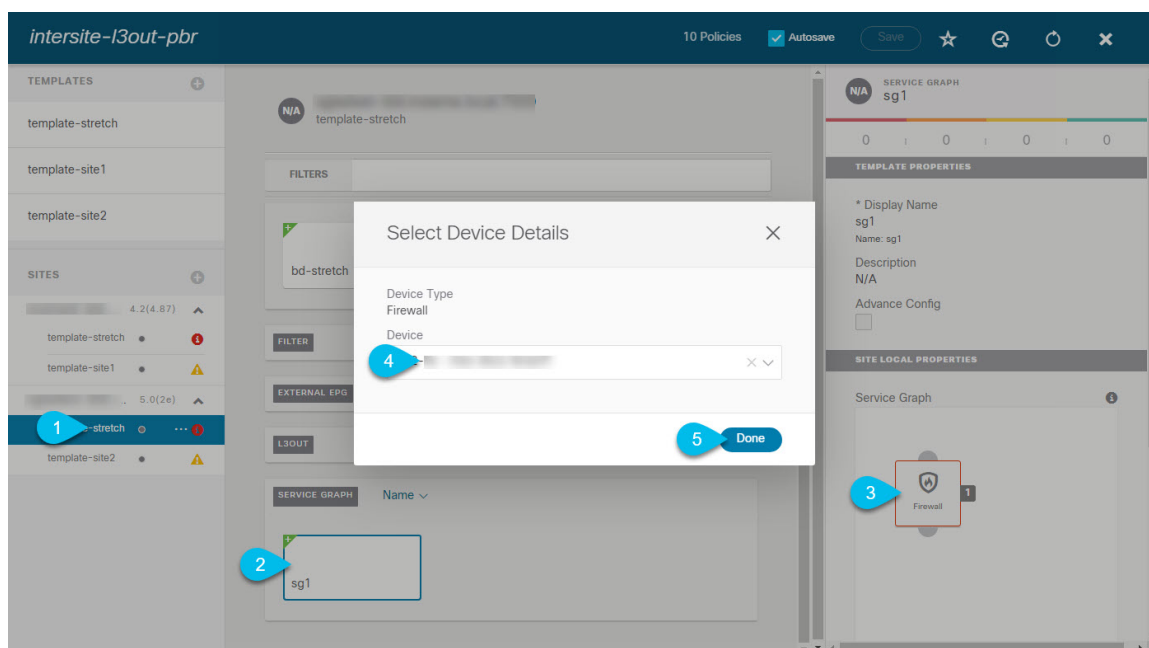
- [契約からのフィルタ (Filters From Contract)] : コントラクトの件名から特定のフィルタを使用します。

- d) 右側のサイドバーで、[サービスノードの定義 (Define Service)]領域までスクロールし、1つ以上のノードを [デバイスのドロップ (Drop Device)] ボックスにドラッグアンドドロップします。

Multi-Siteは、サービス グラフごとに最大2つのノードをサポートします。

ステップ3 サービス グラフのサイトローカル デバイスを設定します。

この手順は、Multi-Site ドメインの一部であるすべてのサイトに対して実行する必要があります。



- 左側のサイドバーから、このサービス グラフを展開するサイトの1つを選択します。
- メイン ペインで、作成したサービス グラフを選択します。
- 右側のサイドバーで、サービス グラフ ノードをクリックします。
- [デバイスの詳細の選択 (Select Device Details)] ウィンドウで、サイトの APIC で作成したデバイスを選択します。

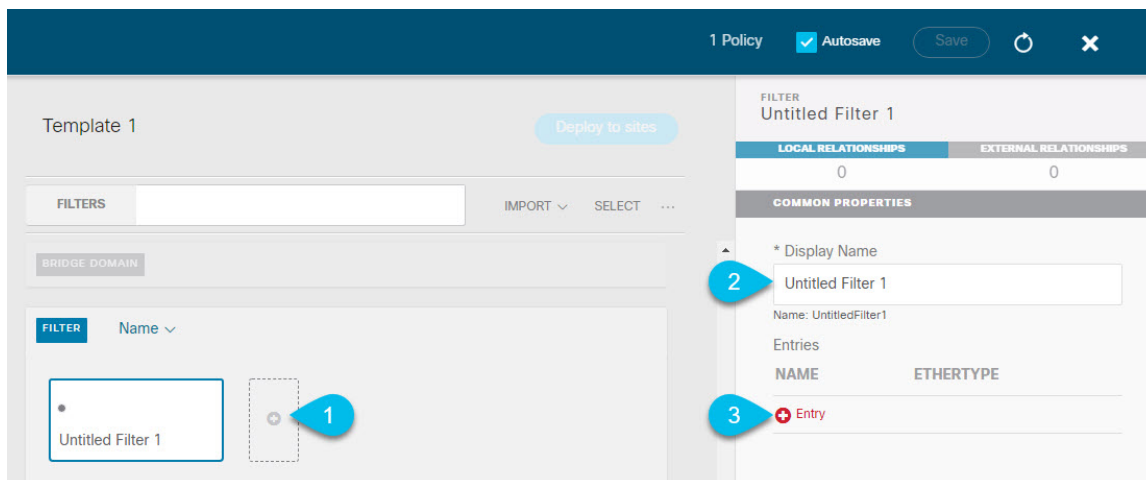
コントラクトのフィルタの作成

次のものがが必要です。

- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

このセクションでは、サービスグラフを介してアプリケーション EPG と L3Out 間のトラフィックに使用されるコントラクトとフィルタの作成方法について説明します。

ステップ1 フィルタを作成します。



- [Filter (フィルタ)]** エリアまでスクロールし、**[+]** をクリックしてフィルタを作成します。
- 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。
- 右側のペインで、**[+ エントリ (+ Entry)]** をクリックします。

ステップ 2 フィルタの詳細を入力します。

Add Entry ×

COMMON PROPERTIES

Name
icmp 1

Description

Ether Type
ip 2

IP Protocol
icmp

Destination port range from
unspecified

Destination port range to
unspecified 3

ON-PREM PROPERTIES

Match only fragments

stateful

ARP flag
unspecified × ▽

Source port range from
unspecified ▽

Source port range to
unspecified ▽

TCP session rules
unspecified × ▽

4 Save

- フィルタの [名前 (Name)] を指定します。
- [イーサタイプ (Ether Type)] と [IP プロトコル (IP Protocol)] を選択します。

■ コントラクトのフィルタの作成

たとえば、[ip] と [icmp] です。

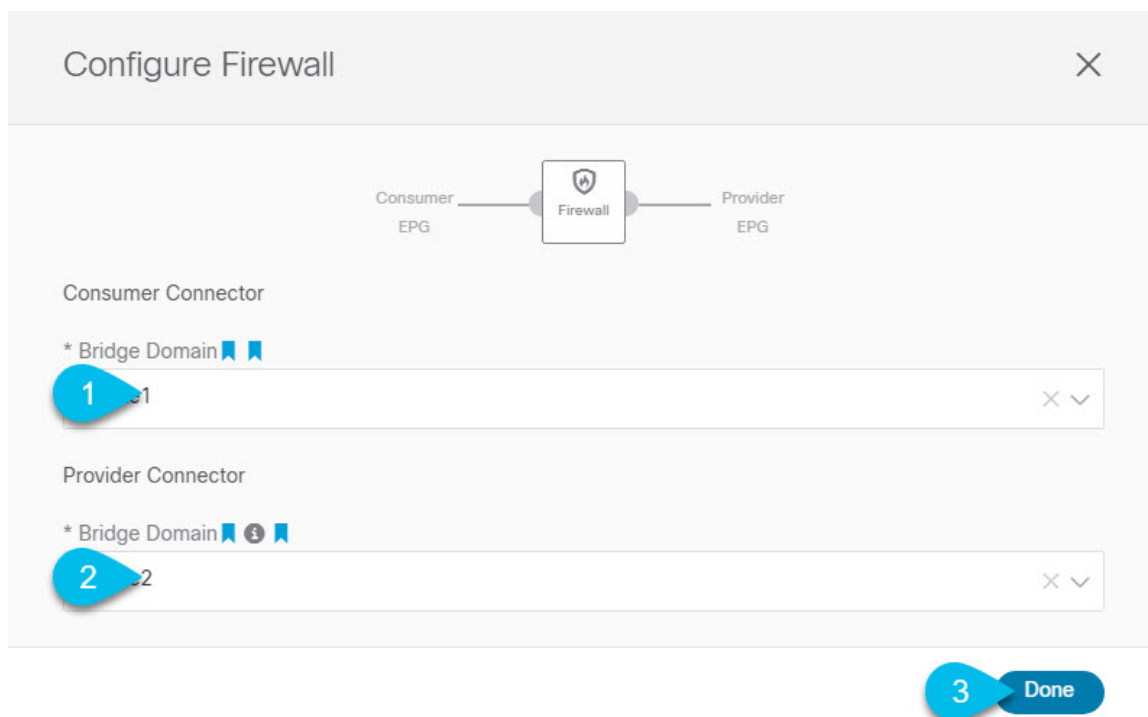
- c) 他のプロパティは [未指定 (unspecified)] のままにします。
- d) **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ3 コントラクトの作成

- a) 中央ペインで、**[コントラクト (Contracts)]** エリアまで下方にスクロールし、**[+]** をクリックして、コントラクトを作成します。
- b) 右側のペインで、コントラクトの **[表示名 (Display Name)]** を入力します。
- c) **[範囲 (Scope)]** ドロップダウンメニューから、コントラクトの範囲を選択します。
アプリケーション EPG と L3Out が同じ VRF にある場合は、[vrf] を選択します。それ以外の場合は、[inter-VRF] 使用例を設定します。
- d) **[両方向に適用 (Apply both directions)]** が有効になっていることを確認します。
これにより、コンシューマからプロバイダへ方向とプロバイダからコンシューマへ方向の両方に同じフィルタを適用できます。

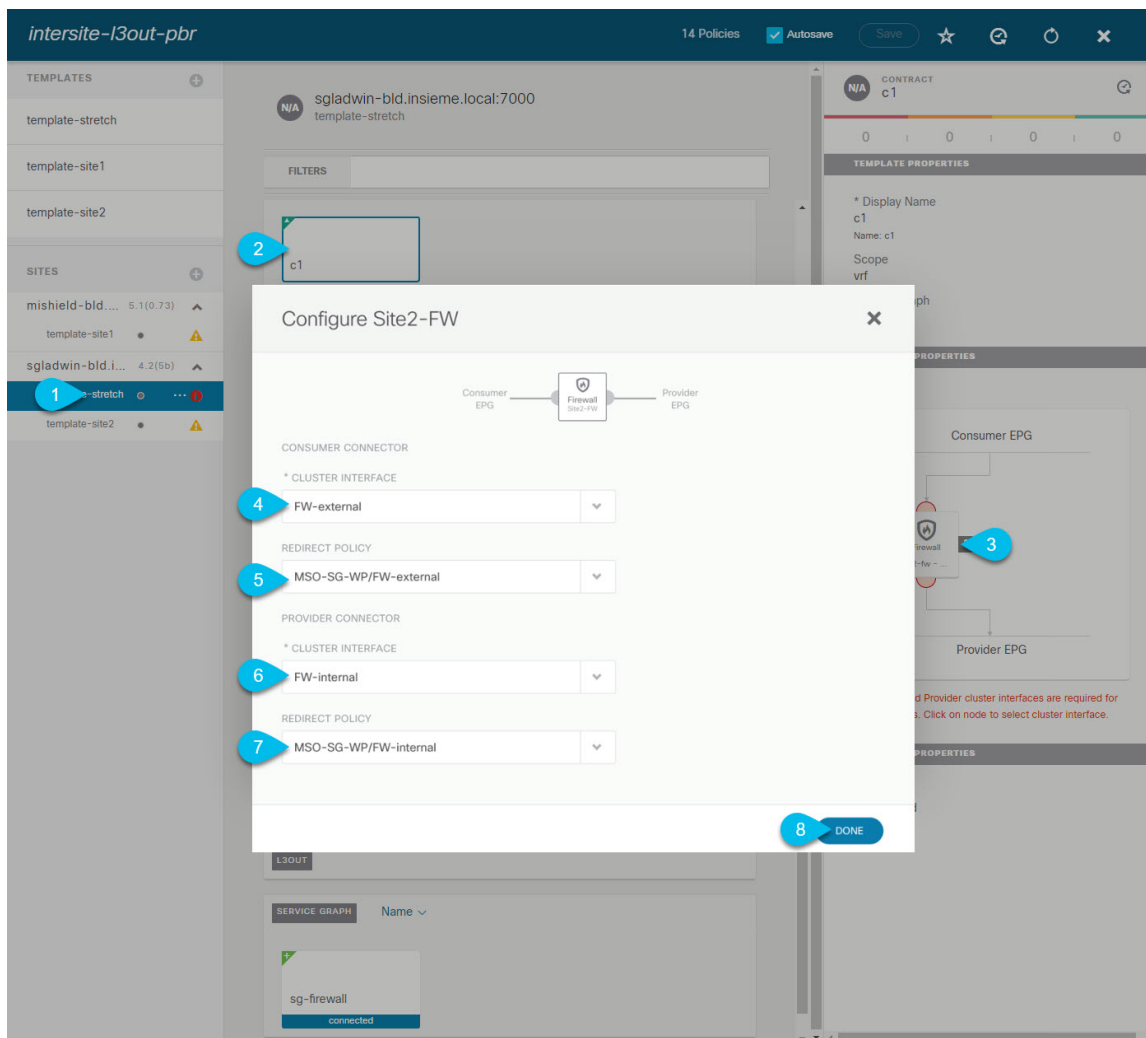
- e) 右側のペインで、**[フィルタ チェーン (Filter Chain)]** 領域までスクロールし、**[+ フィルタ (+ Filter)]** をクリックしてフィルタをコントラクトに追加します。
- 表示される **[フィルタ チェーンの追加 (Add Filter Chain)]** ウィンドウで、**[名前 (Name)]** ドロップダウンメニューから前のセクションで追加したフィルタを選択します。
- コントラクトで **[両方向に適用 (Apply both directions)]** オプションを無効にした場合は、他のフィルタチェーンに対してこの手順を繰り返します。
- f) **[サービス グラフ (Service Graph)]** ドロップダウンから、前のセクションで作成したサービスグラフを選択します。
- g) サービス グラフ ノードをクリックしてコネクタを設定します。

ステップ 4 サービス グラフ ノードのコネクタのブリッジ ドメインを選択します。



- a) **[コンシューマ コネクタ (Consumer Connector)]** ブリッジ ドメインを指定します。
- b) **[プロバイダ コネクタ (Provider Connector)]** ブリッジ ドメインを指定します。
- c) **[完了 (Done)]** をクリックして保存します。

ステップ 5 コントラクトのサイトローカル プロパティを設定します。



- 左側のサイドバーで、割り当て先のサイトの下にあるテンプレートを選択します。
- メイン ペインで、コントラクトを選択します。
- 右側のサイドバーで、サービス グラフ ノードをクリックします。
- [クラスタ インターフェイス (Cluster Interface)] を [コンシューマ コネクタ (Consumer Connector)] として選択します。
- [リダイレクト ポリシー (Redirect Policy)] を [コンシューマ コネクタ (Consumer Connector)] として選択します。
- [クラスタ インターフェイス (Cluster Interface)] を [プロバイダ コネクタ (Consumer Connector)] として選択します。
- [リダイレクト ポリシー (Redirect Policy)] を [プロバイダ コネクタ (Consumer Connector)] として選択します。
- [完了 (Done)] をクリックして、変更内容を保存します。
- すべてのサイトに対してこの手順を繰り返します。

アプリケーション EPG の作成

アプリケーション EPG の VRF およびブリッジ ドメインの作成

ここでは、アプリケーション EPG の VRF およびブリッジ ドメイン (BD) を作成する方法について説明します。

始める前に

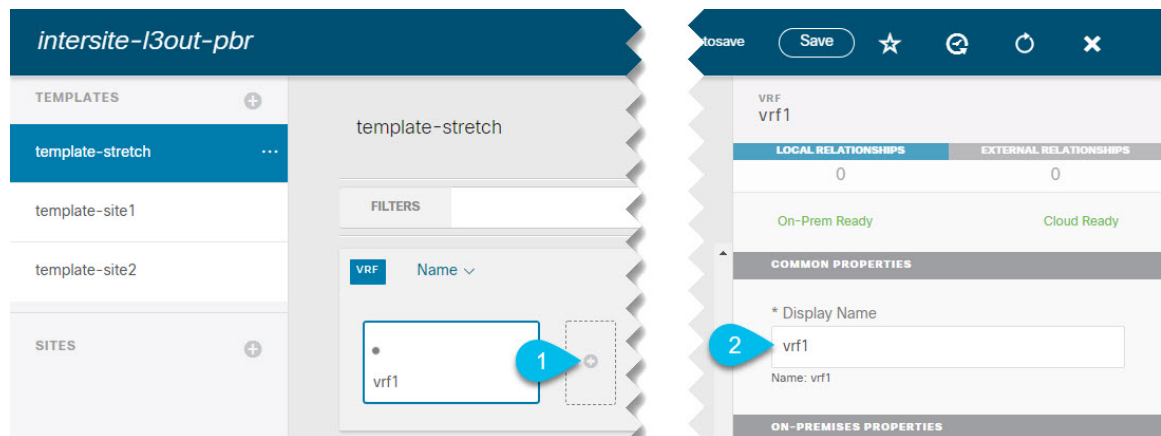
次のものがが必要です。

- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

ステップ 1 VRF および BD を作成するテンプレートを選択します。

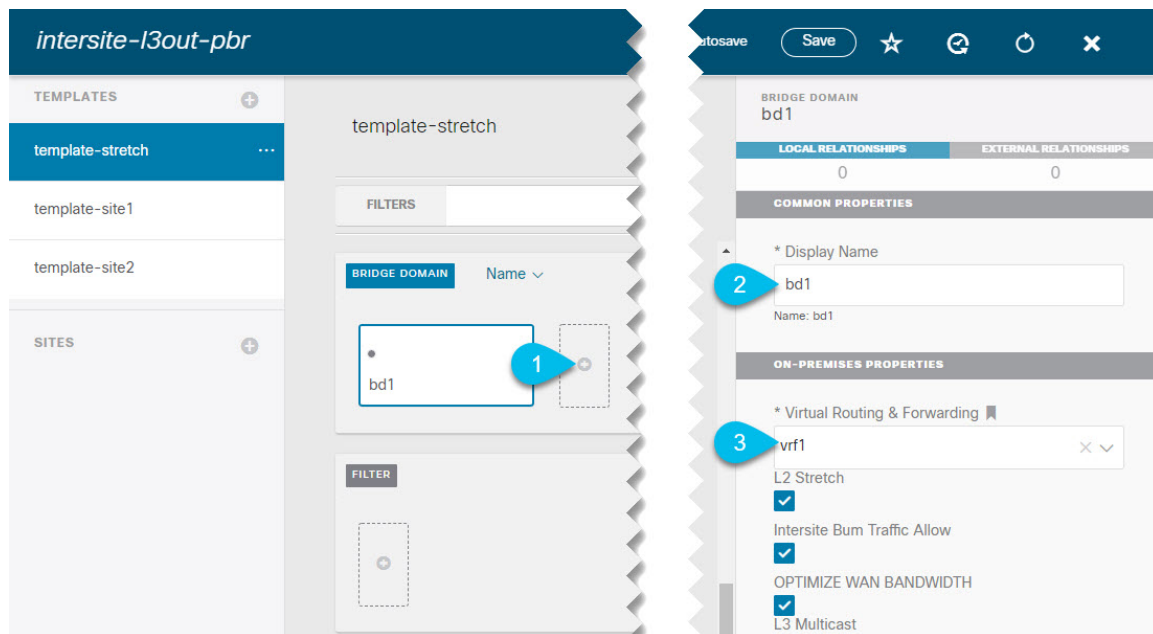
VRF および BD を拡張する場合は、`template-stretch` テンプレートを選択します。それ以外の場合は、サイト固有のテンプレートのいずれかを選択します。

ステップ 2 VRF を作成します。



- メイン ペインの **[VRF]** 領域で、プラス (+) 記号をクリックして VRF を追加します。
- 右側のサイドバーで、フィルタの **[表示名 (Display Name)]** を入力します。
- 展開に対して適切である他の VRF 設定を指定します。

ステップ 3 BD を作成します。



- メイン ペインの **[BD]** 領域で、プラス (+) 記号をクリックしてBDを追加します。
- 右側のサイドバーで、フィルタの **[表示名 (Display Name)]** を入力します。
- [仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップで作成された VRF を選択します。
- 展開に対して適切である他の BD 設定を指定します。

アプリケーション プロファイルと EPG の作成

このセクションでは、サービスグラフでサイト間 L3Out を使用するために後で設定するアプリケーション EPG を作成する方法について説明します。

始める前に

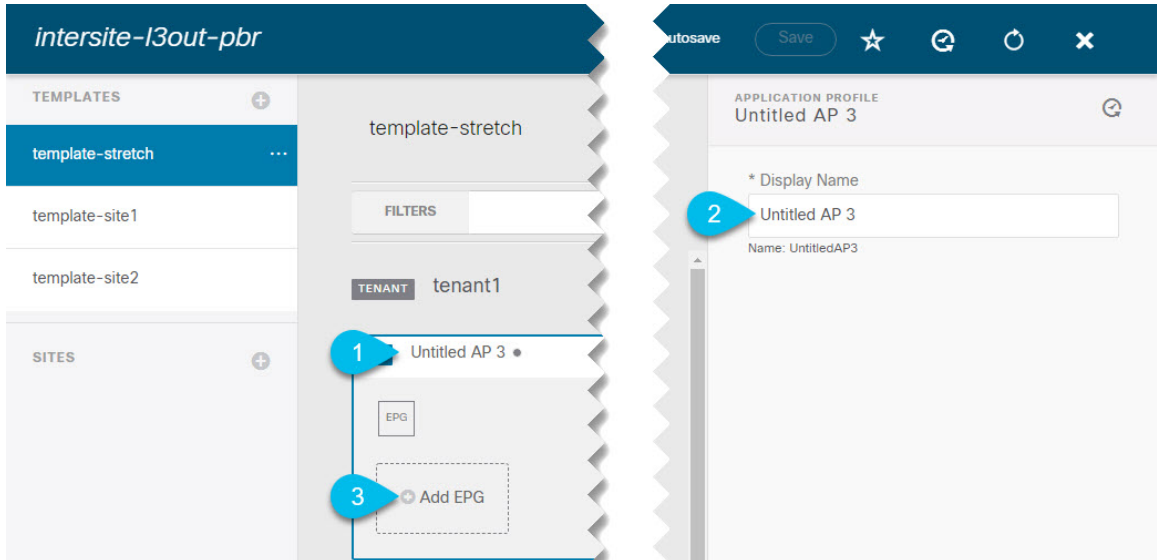
次のものがが必要です。

- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。
- [コントラクトのフィルタの作成 \(251 ページ\)](#) の説明に従って、アプリケーション EPG と外部 EPG の間での通信のために使用するコントラクトを作成していること。
- [アプリケーション EPG の VRF およびブリッジ ドメインの作成 \(257 ページ\)](#) の説明に従って、EPG に使用する VRF と BD を作成していること

ステップ 1 オブジェクトを作成するテンプレートを選択します。

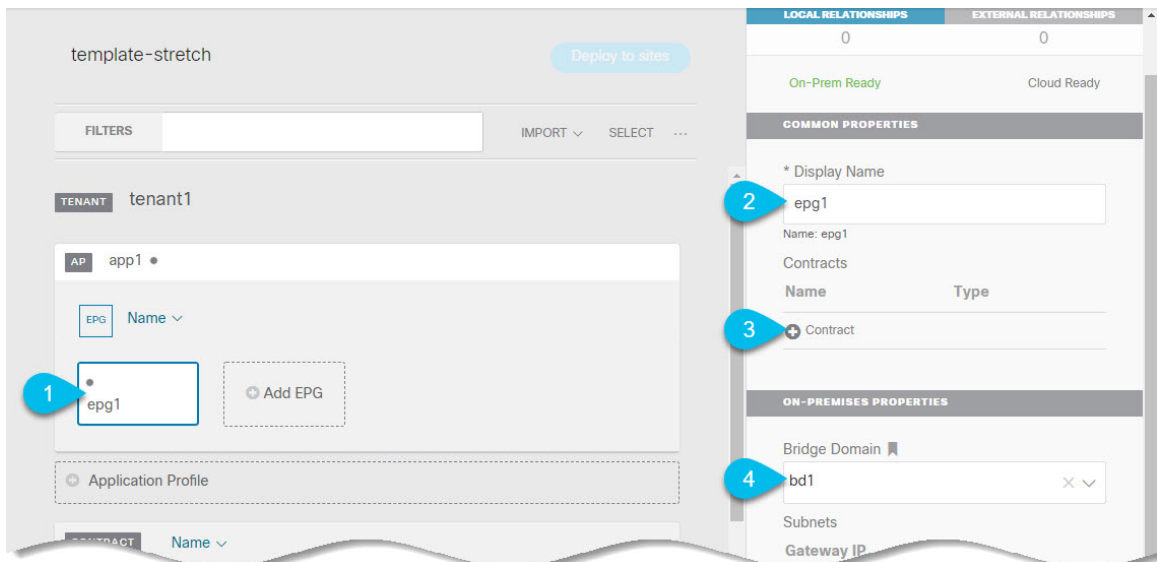
アプリケーション EPG を拡張する場合は、拡張テンプレートで作成します。アプリケーション EPG をサイトローカルにする場合は、サイト固有のテンプレートで作成します。

ステップ 2 アプリケーション プロファイルと EPG を作成します。



- メイン ペインで、[+ アプリケーション プロファイル (+ Application profile)] をクリックします。
- 右側のサイドバーで、プロファイルの [表示名 (Display Name)] を入力します。
- メイン ペインで、[+ EPG の追加 (+Add EPG)] をクリックします。

ステップ 3 EPG を設定します。



- メイン ペインで、アプリケーション EPG を選択します。
- 右側のサイドバーで、EPG の [表示名 (Display Name)] を入力します。
- [+ コントラクト (+Contract)] をクリックし、コントラクトを選択します。
EPG 通信用に作成したコントラクトを選択し、そのタイプを設定します。

アプリケーション EPG と L3Out 外部 EPG に同じ VRF を使用している場合は、どちらかをコンシューマまたはプロバイダーとして選択できます。ただし、それらが異なる VRF にある場合は、アプリケーション EPG のコントラクトタイプにコンシューマを選択する必要があります。

- d) [ブリッジドメイン (Bridge Domain)] ドロップダウンで、BD を選択します。
- e) 展開に適した他の EPG 設定を指定します。

L3Out 外部 EPGの作成

サイト間 L3Out および VRF の作成またはインポート

ここでは、L3Out を作成し、それを Nexus Dashboard Orchestrator (NDO) GUI で VRF に関連付ける方法について説明します。これは APIC サイトにプッシュされるか、または APIC サイトの 1 つから既存の L3Out をインポートします。次に、この L3Out を外部 EPG に関連付け、その外部 EPG を使用して特定のサイト間 L3Out の使用例を設定します。



- (注) L3Out に割り当てる VRF は、任意のテンプレートまたはスキーマにすることができますが、L3Out と同じテナントに存在する必要があります。

始める前に

次のものがが必要です。

- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。

ステップ 3 [スキーマ (schema)] を選択し、VRF と L3Out を作成またはインポートするテンプレートを選択します。

複数のサイトに関連付けられているテンプレートで L3Out を作成すると、L3Out がそれらすべてのサイトに作成されます。1 つのサイトに関連付けられているテンプレートで L3Out を作成すると、そのサイトでのみ L3Out が作成されます。

ステップ 4 新しい VRF と L3Out を作成します。

既存の L3Out をインポートする場合は、この手順をスキップします。

- (注) NDO で L3Out オブジェクトを作成し、それを APIC にプッシュすることはできませんが、L3Out の物理設定は APIC で実行する必要があります。

- a) [VRF] エリアまで下にスクロールし、+ アイコンをクリックして新しい VRF を追加します。
右側のサイドバーで、VRF の名前を入力します (例: vrf-l3out)。
- b) [L3Out] 領域まで下にスクロールし、+ アイコンをクリックして新しい L3Out を追加します。
右側のスライダで、必要な情報を入力します。
- c) L3Out の名前を指定します (例: l3out-intersite)。
- d) [仮想ルーティングと転送 (Virtual Routing & Forwarding)] ドロップダウンから、前のステップで作成された VRF を選択します。

ステップ 5 既存の L3Out をインポートします。

前の手順で新しい L3Out を作成した場合は、この手順をスキップします。

メインテンプレートビューの上部で [インポート (Import)] をクリックし、インポート元のサイトを選択します。

The screenshot shows the 'Import from Site7' dialog box. On the left, there is a list of policy types with their counts: APPLICATION PROFILE (0 out of 1), EPG (0 out of 7), EXTERNAL EPG (0 out of 1), CONTRACT (0 out of 5), FILTER (0 out of 2), VRF (1 out of 3), and BD (0 out of 15). At the bottom of this list, 'L3OUT' is highlighted with a blue bar and a '1' in a blue circle. On the right, the 'SELECT TO IMPORT' section has a search icon and an 'INCLUDE RELATIONS' toggle (turned on, with a '3' in a blue circle). Below this, a table shows one selected VRF with a checkmark and a '2' in a blue circle. At the bottom right, there is a blue 'Import' button with a '4' in a blue circle.

- a) [インポート (Import)] ウィンドウの [ポリシー タイプ(Policy Type)] メニューで、[L3Out] を選択します。
- b) インポートする L3Out をチェックします。
- c) (オプション) L3Out に関連付けられているすべてのオブジェクトをインポートする場合は、[関係を含める (Include Relationships)] ノブを有効にします。
- d) [Import] をクリックします。

外部 EPG の設定

このセクションでは、サイト間 L3Out と関連付ける外部 EPG の作成方法について説明します。その後、この外部 EPG とコントラクトを使用すれば、あるサイトのエンドポイント用の特定のユースケースを設定し、別のサイトの L3Out を使用することができます。

始める前に

次のものがが必要です。

- [テンプレートの作成 \(248 ページ\)](#) の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。
- [サイト間 L3Out および VRF の作成またはインポート \(260 ページ\)](#) の説明に従って作成された、またはインポートされた L3Out と VRF。

ステップ 1 外部 EPG を作成するテンプレートを選択します。

複数のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、それらすべてのサイト上で作成されます。単一のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、そのサイト内でのみ作成されます。

ステップ 2 [外部 EPG (External EPG)] エリアまで下方にスクロールして、+ アイコンをクリックして外部 EPG を追加します。

右側のスライダで、必要な情報を入力します。

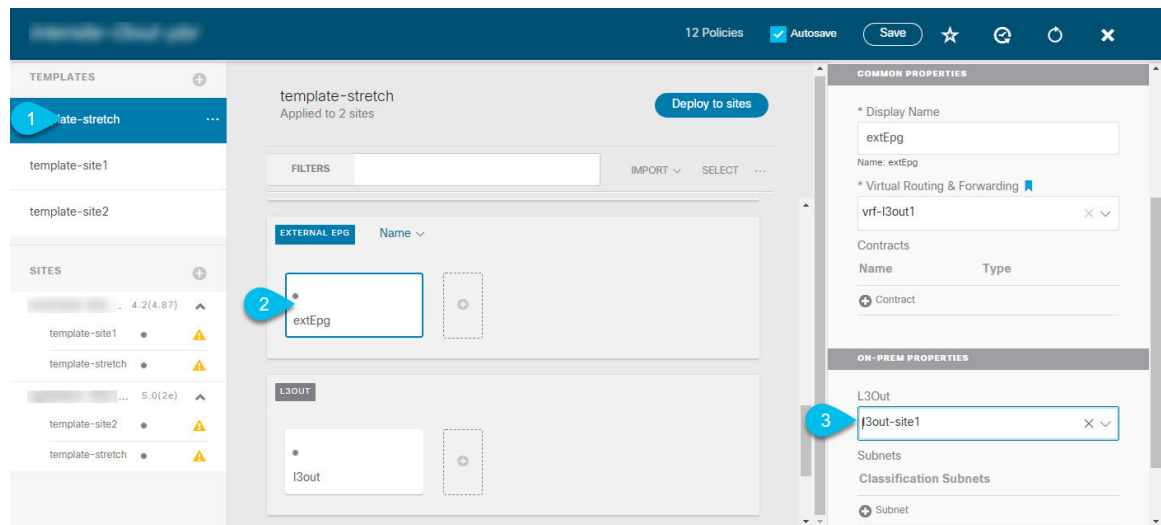
- a) 外部 EPG の名前を入力します。たとえば extEpg のようにします。
- b) [仮想ルーティングと転送 (Virtual Routing & Forwarding)] ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。
- c) [+コントラクト (+Contract)] をクリックし、コントラクトを選択します。

EPG 通信用に作成したコントラクトを選択し、そのタイプを設定します。

アプリケーション EPG と L3Out 外部 EPG に同じ VRF を使用している場合は、どちらかをコンシューマまたはプロバイダとして選択できます。ただし、それらが異なる VRF にある場合は、外部 EPG のコントラクトタイプのプロバイダを選択する必要があります。

ステップ 3 L3Out をテンプレート レベルで割り当てるには...

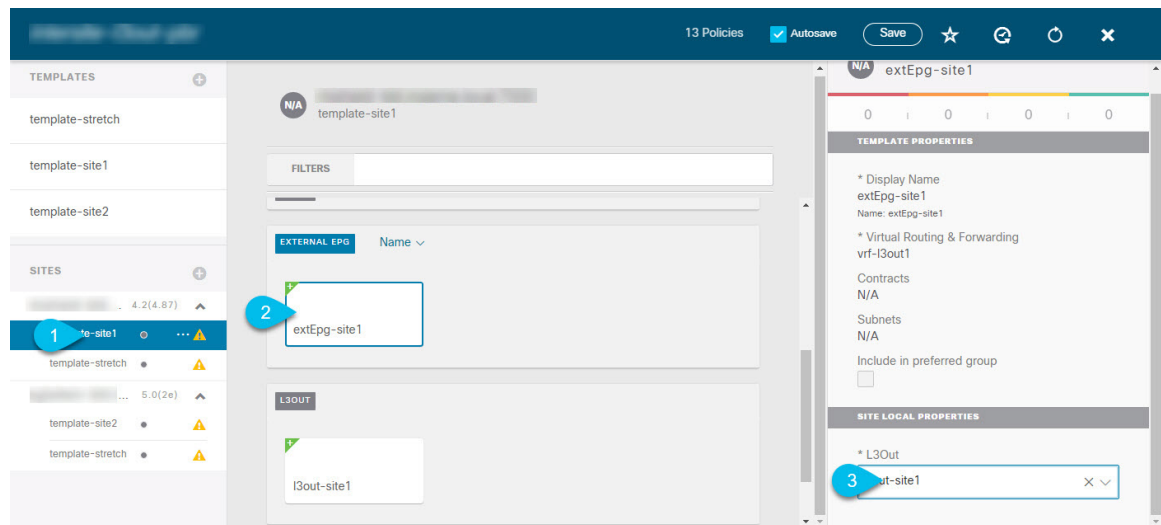
外部 EPG 用の L3Out は、テンプレートレベルで選択し、設定できます。その場合、L3Out をサイトローカル レベルで設定することはできません。



- スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。
- [外部 EPG (External EPG)] エリアまで下方にスクロールして、外部 EPG を選択します。
- 右サイドバーで、[L3Out] ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

ステップ 4 L3Out をサイトローカル レベルで割り当てるには...

代わりに、L3Out をサイトローカル レベルで外部 EPG に関連付けることもできます。



- スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。
- [外部 EPG (External EPG)] エリアまで下方にスクロールして、外部 EPG を選択します。
- 右サイドバーで、[L3Out] ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

この場合、APIC で管理されている L3Out と、オーケストレーションで管理されている L3Out の両方が選択できます。前のセクションでこの目的のため特に作成した L3Out、またはサイトの APIC 内にすでにある L3Out のいずれかを選択します。



第 22 章

レイヤ 3 マルチキャスト

- レイヤ 3 マルチキャスト (265 ページ)
- レイヤ 3 マルチキャストルーティング (266 ページ)
- ランデブー ポイント (267 ページ)
- マルチキャスト フィルタ処理 (268 ページ)
- Layer 3 マルチキャストに関するガイドラインと制限事項 (269 ページ)
- マルチキャスト ルート マップ ポリシーの作成 (271 ページ)
- Any-Source Multicast (ASM) マルチキャストの有効化 (272 ページ)
- ソース固有マルチキャスト (SSM) の有効化 (274 ページ)

レイヤ 3 マルチキャスト

Cisco マルチキャスト レイヤ 3 マルチキャストは、VRF、ブリッジドメイン (BD)、およびマルチキャスト ソースが存在している任意の EPG という、3 つのレベルで有効または無効にできます。

トップ レベルでは、マルチキャスト ルーティングは、任意のマルチキャストが有効な BD を持つ VRF で有効にする必要があります。マルチキャストが有効な VRF では、マルチキャストが有効な BD と、マルチキャストルーティングが無効な BD の組み合わせにすることができます。Cisco Nexus Dashboard Orchestrator GUI で VRF のマルチキャスト ルーティングを有効にすると、VRF が拡張されている APIC サイトで有効になります。

いったんマルチキャストで VRF を有効にすると、VRF の下の個別の BD では、マルチキャストルーティングを有効にすることができます。BD でレイヤ 3 マルチキャストを設定すると、その BD 上では、プロトコル独立ルーティング (PIM) が有効になります。デフォルトでは、PIM はすべての BD で無効になっています。

特定のサイトローカル EPG に属するソースがリモートサイトにマルチキャストトラフィックを送信する場合、Nexus Dashboard Orchestrator はシャドウ EPG を作成し、ソース EPG のリモートサイトで対応するサブネットルートをプログラムする必要があります。リモート Top-of-Rack (TOR) スイッチに適用される設定変更を制限するには、マルチキャスト送信元が存在するローカル EPG でレイヤ 3 マルチキャストを明示的に有効にする必要があります。これにより、これらの EPG に必要な設定のみがリモートサイトにプッシュされます。マルチキャストの受信者が存在する EPG では、レイヤ 3 マルチキャストを有効にする必要はありません。

マルチサイトは、以下のレイヤ3 マルチキャスト送信元と受信者のすべての組み合わせをサポートしています。

- ACI ファブリック内のマルチキャスト送信元と受信者
- ACI ファブリック外のマルチキャスト送信元と受信者
- ACI ファブリック内のマルチキャスト送信元と外部受信者
- ACI ファブリック内のマルチキャスト受信者と外部送信元

レイヤ3 マルチキャスト ルーティング

次に示すのは、サイト間レイヤ3 マルチキャスト ルーティングの高レベルでの概要です。

- マルチキャスト送信元がエンドポイント (EP) として ACI ファブリックに1つのサイトで接続され、マルチキャストフローのストリーミングを開始すると、送信元 VRF の指定フォワーダとして選択された特定のサイトのスパインスイッチは、すべてのリモートサイトにマルチキャストトラフィックを転送します。これらのサイトでは、ヘッドエンドレプリケーション (HREP) を使用してソースの VRF がストレッチされます。特定のリモートサイトにその特定のグループのレシーバが存在しない場合、トラフィックは受信スパインノードでドロップされます。少なくとも1つのレシーバがある場合、トラフィックはサイトに転送され、すべてのリーフノードに到達します。ここでは VRF が展開されており、その時点でのグループメンバーシップ情報に基づいてプルーニング/転送が行われます。
- Cisco ACI リリース 5.0(1) よりも前では、マルチキャスト ルーティング ソリューションは、外部マルチキャストルータが、PIM-SM エニソース マルチキャスト (ASM) が展開されたランデブーポイント (RP) である必要がありました。それぞれのサイトは、指定された拡張 VRF に対し、同じ RP アドレスをポイントしている必要があります。RP は、サイトローカルの L3Out を介して、各サイトに到達できる必要があります。
- 送信元がファブリックの外側、受信者が内側にある場合、受信者は、RP に対する PIM ジョインとしてのサイトローカルの L3Out を介してトラフィックをプルします。送信元は常にサイトローカルの L3Out を介して送信されます。
- 各サイトの受信者には、外部の送信元からのトラフィックを、サイトローカルの L3Out を介して取り込むことが期待されます。そのため、あるサイトの L3Out で受信したトラフィックを他のサイトに送信することはできません。このことは、スパインにおいて、HREP トンネルへ複製中のマルチキャストトラフィックをプルーニングすることによって行われません。

これを可能にするために、外部送信元から発信され、ローカル L3Out で受信されるすべてのマルチキャストトラフィックは、外部 VXLAN ヘッダーの特別な DSCP 値で再マーキングされます。スパインはその特定の DSCP 値と一致するため、トラフィックがリモートサイトに複製されることはありません。

- サイトに接続された送信元から発信されたトラフィックは、ローカル L3Out またはリモートサイトに展開された L3Out を介して外部レシーバに送信できます。これに使用される

特定の L3Out は、外部ネットワークからその特定のマルチキャストグループの PIM Join を受信したサイトにも依存します。

- BD と Nexus Dashboard Orchestrator 上の EPG でマルチキャストが有効にされている場合、BD のすべてのサブネットは、境界リーフ (BL) ノードを含めて、すべてのリーフスイッチのルーティングテーブルにプログラミングされます。これにより、リーフスイッチにアタッチされた受信者は、送信側 BD がリーフスイッチに存在しない場合に、マルチキャストソースの到達可能性を判定することができます。BL に対して適切なポリシーが設定されていた場合、サブネットは外部ネットワークにアドバタイズされます。ホストベースのルーティングが BD で設定されている場合、/32 ホストルートがアドバタイズされます。

マルチキャストルーティングについての詳細は、[IP マルチキャスト](#)のセクションを参照してください。これは *Cisco APIC* レイヤ 3 ネットワーク コンフィギュレーションガイドに記されています。

ランデブーポイント

マルチキャストトラフィックソースは、マルチキャストアドレスグループにパケットを送信し、そのグループに参加するすべてのユーザーがパケットを受信できるようにします。1つまたは複数のグループからのトラフィックを受信する受信者は、通常は **Internet Group Management Protocol (IGMP)** を使用して、グループへの参加を要求できます。受信者がグループに参加するたびに、そのグループに対してマルチキャスト配信ツリーが作成されます。ランデブーポイント (RP) は、PIM-SM マルチキャストドメイン内にあるルータで、マルチキャスト共有ツリーの共有ルートとして動作します。

ネットワークに冗長 RP 機能を提供する一般的な方法は、ネットワーク内の 2 つ以上の RP が同じユニキャスト IP アドレスを共有できるようにする、ユニキャスト RP と呼ばれる機能を導入することです。これにより、冗長性とロードバランシングが提供されます。1つの RP デバイスに障害が発生した場合、他の RP はサービスを中断せずに引き継ぐことができます。マルチキャストルータは、ネットワーク内のユニキャスト RP のいずれかに接続して、最も近い RP に転送される join 要求を使用して、マルチキャスト共有ツリーに参加することもできます。

Nexus Dashboard Orchestrator では、次の 2 種類の RP 設定がサポートされています。

- **静的 RP**—RP が ACI ファブリックの外部にある場合。
- **ファブリック RP** : ACI ファブリック内の境界リーフスイッチがユニキャスト RP として機能する場合。

任意の数のルータを RP として機能するように設定できます。また、異なるグループ範囲をカバーするようにそれらを設定できます。ACI ファブリック内部で RP を定義する場合には、グループのリストを含むルートマップポリシーを作成し、それを VRF に追加するときこのポリシーを RP にアタッチすることで、RP がカバーするグループを設定できます。ルートマップの作成については [マルチキャストルートマップポリシーの作成 \(271 ページ\)](#) で説明しており、VRF の設定については [Any-Source Multicast \(ASM\) マルチキャストの有効化 \(272 ページ\)](#) で説明しています。

スタティック RP とファブリック RP の両方で、マルチキャストルーティングが有効になっている VRF に PIM 対応境界リーフ スイッチが必要です。L3Out の設定は、L3Out の PIM の有効化を含め、各サイトの APIC から現在ローカルに設定されています。L3Out での PIM の設定の詳細については、[Cisco APIC Layer 3 Networking Configuration Guide](#)を参照してください。

マルチキャスト フィルタ処理

マルチキャストフィルタリングは、Cisco APIC リリース 5.0(1) および Nexus Dashboard Orchestrator リリース 3.0(1) 以降で使用可能なマルチキャスト トラフィックのデータプレーンフィルタリング機能です。

Cisco APIC は、誰がマルチキャスト フィードを受信でき、どのソースから受信できるかを制御するために使用できるコントロールプレーン構成をサポートしています。一部の展開で、データプレーン レベルでマルチキャスト ストリームの送信および/または受信を制限することが望ましい場合があります。たとえば、LAN 内のマルチキャスト送信者が特定のマルチキャストグループにのみ送信できるようにするか、受信者が特定の送信元からのみマルチキャストを受信できるようにする必要がある場合があります。

Nexus Dashboard Orchestrator からのマルチキャスト フィルタリングを構成するには、送信元と宛先のマルチキャスト ルート マップを作成します。それぞれのマップには、マルチキャスト トラフィックの送信元 IP および/またはアクション (許可 (Permit) または 拒否 (Deny)) が関連付けられたグループに基づく 1 つ以上のフィルタ エントリが含まれています。次に、ルートマップをブリッジ ドメインにアタッチして、ブリッジ ドメインでフィルタリングを有効にします。

マルチキャスト ルート マップを作成すると、1 つ以上のフィルタ エンティティを定義できます。一部のエントリは許可 (Permit) アクションで設定でき、その他のエントリは拒否 (Deny) アクションで設定できます。すべてが同じルートマップ内で行われます。各エントリに対して、**送信元 IP** と **グループ IP** を提供して、フィルタに一致するトラフィックを定義できます。これらのフィールドの少なくとも 1 つを提供できますが、両方を含むことを選択できます。フィールドの 1 つが空白のままの場合は、すべての値と一致します。

マルチキャスト送信元フィルタリングとマルチキャスト受信先フィルタリングの両方を同じブリッジ ドメインで有効にできます。この例では、1 つのブリッジ ドメインが送信元のみならず、受信先の両方に対してフィルタ処理を提供できます。

BD に対してルート マップを提供しない場合、デフォルトアクションはブリッジ ドメインですべてのマルチキャスト トラフィックを許可することです。しかし、ルートマップを選択する場合、デフォルトアクションはルート マップのフィルタ エントリに明示的に一致しないトラフィックを拒否するように変更されます。

送信元のフィルタ処理

ブリッジドメインでトラフィックを送信する任意のマルチキャストソースの場合、1 つ以上の送信元とグループ IP フィルタが定義されているルート マップ ポリシーを設定できます。次に、トラフィックはルートマップのすべてのエントリと照合され、次のいずれかのアクションが実行されます。

- トラフィックがルートマップの許可 (Permit) アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはそのソースからそのグループへのトラフィックを許可します。
- トラフィックがルートマップの拒否 (Deny) アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはそのソースからそのグループへのトラフィックを拒否します。
- トラフィックがルートマップの任意のエントリと一致しない場合、デフォルトの拒否 (Deny) アクションが適用されます。

送信元フィルタは、送信元が接続されている ACI リーフノードで表されるファーストホップルータ (FHR) のブリッジドメインに適用されます。フィルタは、異なるブリッジドメイン内の受信先、同じブリッジドメイン内の受信先、および外部受信先がマルチキャストを受信するのを防ぎます。

宛先(受信先)フィルタ処理

宛先(受信先)フィルタ処理は、受信先がマルチキャスト処理グループに参加することを妨げません。マルチキャストトラフィックは、代わりに、送信元 IP とマルチキャストグループの組み合わせに基づいて、データプレーンで許可またはドロップされます。

送信元フィルタ処理と同様に、マルチキャストトラフィックが宛先フィルタと一致するとき、次のアクションの一つが起きます。

- トラフィックがルートマップの許可 (Permit) アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはその送信元から受信先へのトラフィックを許可します。
- トラフィックがルートマップの拒否 (Deny) アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはその送信元から受信先へのトラフィックを拒否します。
- トラフィックがルートマップの任意のエントリと一致しない場合、デフォルトの拒否 (Deny) アクションが適用されます。

宛先フィルタは、ACI リーフノードが代表する、ラストホップルーター (LHR) 上のブリッジドメインに適用されるため、その他のブリッジドメインはマルチキャストトラフィックを引き続き受信できます。

Layer 3 マルチキャストに関するガイドラインと制限事項

現在のソフトウェアリリースまでは、Cisco Nexus Dashboard Orchestrator を使用して、IGMP または PIM 関連のポリシーなどの特定のマルチキャストコントロールプレーンフィルタリングポリシーを各サイトに展開することはできません。したがって、エンドツーエンドソリューションが機能するためには、各 APIC サイトでの使用例に必要な追加ポリシーを個別に設定する必要があります。各サイトでこれらの設定を構成する方法の詳細については、『[CISCO APIC Layer 3 Network Configuration Guide](#)』を参照してください。

また、すべてのファブリックの QoS DSCP 変換ポリシーが一貫して設定されていることを確認する必要があります。ACI ファブリックでカスタム QoS ポリシーを作成する場合、ACI QoS レベルと、ファブリックに出入りするパケットのパケットヘッダー DSCP 値との間のマッピングを作成できます。マルチキャストトラフィックがサイト間を通過するには、すべてのサイトで同じ ACI QoS レベルを同じ DSCP 値にマッピングする必要があります。各サイトでこれらの設定を構成する方法の詳細については、[CISCO APIC and QoS](#) を参照してください。

マルチキャストフィルタ処理

マルチキャストフィルタ処理を有効にすると、次の追加のガイドラインが適用されます。

- マルチキャストフィルタ処理は、IPv4 でのみサポートされています。
- 同じブリッジドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。
- ブリッジドメインにマルチキャストフィルタを設定しない場合は、そのブリッジドメインで送信元フィルタまたは宛先フィルタルートマップを設定しないでください。

デフォルトでは、ルートマップはブリッジドメインに関連付けられていません。これは、すべてのマルチキャストトラフィックが許可されることを意味します。ルートマップがブリッジドメインに関連付けられている場合、そのルートマップ内の **permit** エントリだけが許可され、その他のすべてのマルチキャストトラフィックはブロックされます。

空のルートマップをブリッジドメインに接続すると、ルートマップはデフォルトで **deny all** を想定するため、すべての送信元とグループがそのブリッジドメインでブロックされます。

- マルチキャストフィルタリングは BD レベルで実行され、BD 内のすべての EPG に適用されます。そのため、同じ BD 内の異なる EPG に対して異なるフィルタリングポリシーを設定することはできません。EPG レベルでより詳細にフィルタリングを適用する必要がある場合は、EPG を個別の BD に設定する必要があります。
- マルチキャストフィルタ処理は、任意の送信元マルチキャスト (ASM) 範囲にのみ使用することを目的としています。Source-Specific Multicast (SSM) は送信元フィルタリングではサポートされず、受信者フィルタリングでのみサポートされます。
- 送信側と受信側両方のフィルタ処理の場合、ルートマップエントリはエントリの指定された順序に基づいて照合され、最も小さい番号が最初に一致します。これは、より低い順序のエントリが、リスト内で最長一致でない場合でも、最初に一致することを意味し、より高い順序のエントリは考慮されません。

たとえば、192.0.3.1/32 ソースに対して次のルートマップがあるとします。

順位	送信元 IP	アクション
1	192.0.0.0/16	Permit
2	192.0.3.0/24	拒否

2番目のエントリ (192.0.3.0/24) が送信元 IP と一致する場合でも、最初のエントリ (192.0.0.0/16) は、下位の番号が原因で照合されます。

マルチキャストルートマップポリシーの作成

このセクションでは、マルチキャストルートマップポリシーを作成する方法について説明します。ルートマップを作成する理由としては、次のものが考えられます。

- マルチキャストソースフィルタリングのためにフィルタのセットを定義する。
- マルチキャストデスティネーションフィルタリングのためにフィルタのセットを定義する。
- ランデブーポイント (RP) のためのグループ IP のセットを定義する。

VRF 用の RP を設定する場合、ルートマップを指定しなければ、RP はその VRF のすべてのマルチキャストグループ範囲 (224.0.0.0/4) に合わせて定義されます。または、定義済みのグループまたはグループ範囲を持つルートマップを指定して、RP をそのグループのみに制限することができます。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [メインメニュー (Main menu)] で、[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] を選択します。

ステップ 3 メインペインで、[ポリシーの追加 (Add Policy)] > [マルチキャストルートマップポリシーの作成 (Create Multicast Route-Map Policy)] を選択します。

ステップ 4 [マルチキャストルートマップポリシーの追加 (Add Multicast Route-Map Policy)] 画面で、テナントを選択し、ポリシーの名前を指定します。

ステップ 5 ルートマップエントリを追加するには、[ルートマップエントリの順序 (Route-Map Entry Order)] の下の [ルートマップエントリの追加 (Add Route-Map Entry)] をクリックします。

a) [順序 (Order)] と [アクション (Action)] を指定します。

各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです。

順序は、ルールを評価する順序を決定するために用いられます。

[アクション (Action)] は、一致が検出された場合に実行するアクション (許可 (permit) または拒否 (deny)) を定義します。

b) 必要に応じて、[グループ IP (Group IP)]、[ソース IP (Source IP)]、および [RP IP] 情報を指定します。

このセクションの初めで説明したように、同じマルチキャストルートマップのポリシー UI は 2 つの方法で使用できます。マルチキャストトラフィックのフィルタのセットを設定すること、またはランデブーポイントの設定をマルチキャストグループの特定のセットに制限することです。設定する使用例によっては、この画面のフィールドの一部だけを指定すればよい場合もあります。

- マルチキャストフィルタリングの場合には、フィルタを定義するために、[ソース IP (Source IP)] と [グループ (Group IP)] フィールドを使用します。これらのフィールドの少なくとも1つを提供できますが、両方を含むことを選択できます。フィールドの1つが空白のままの場合は、すべての値と一致します。

グループ IP の範囲は 224.0.0.0 ~ 239.255.255.255 で、ネットマスクは /8 ~ /32 である必要があります。サブネットマスクを指定する必要があります。

RP IP (ランデブーポイントの IP) は、マルチキャストフィルタリングルートマップでは使用しないので、このフィールドはブランクのままにします。

- ランデブーポイントの設定では、[グループ IP (Group IP)] フィールドを使用して RP のマルチキャストグループを定義できます。

グループ IP の範囲は 224.0.0.0 ~ 239.255.255.255 で、ネットマスクは /8 ~ /32 である必要があります。サブネットマスクを指定する必要があります。

ランデブーポイント設定の場合、**RP IP** は RP 設定の一部として設定されます。ルートマップをグループフィルタリングに使用する場合は、ルートマップに **RP IP** アドレスを設定する必要はありません。この場合には、[**RP IP**] と [ソース IP (Source IP)] フィールドを空白のままにします。

- c) エントリを保存するには、[保存 (Save)] をクリックします。

ステップ 6 (オプション) 同じルートポリシーに複数のエントリを追加する場合は、前の手順を繰り返します。

ステップ 7 [保存 (Save)] をクリックして、ルートマップポリシーを保存します。

Any-Source Multicast (ASM) マルチキャストの有効化

以下の手順では、Nexus Dashboard Orchestrator GUI を使用して、VRF、BD、および EPG で ASM マルチキャストを有効にする方法を説明しています。SSM マルチキャストを有効にする場合は、代わりに [ソース固有マルチキャスト \(SSM\) の有効化 \(274 ページ\)](#) の手順に従います。

始める前に

- [Layer 3 マルチキャストに関するガイドラインと制限事項 \(269 ページ\)](#) で説明されている情報を読んで、従っていることを確認してください。
- マルチキャストのフィルタリングを有効にする予定の場合には、[マルチキャストルートマップポリシーの作成 \(271 ページ\)](#) で説明されているように、必要なマルチキャストルートマップを作成します。
- ファブリック RP が有効になっている場合、VRF でサイトローカル L3Out の PIM を有効にする必要があります。

これについては、次の手順のステップ 6 で説明します。L3Out 上での PIM の設定の詳細については、[Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のサイドバーから、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] ビューを選択します。

ステップ 3 変更するスキーマをクリックします。

ステップ 4 VRD でレイヤ 3 マルチキャストを有効にします。

まず、サイト間で拡張されている VRF でレイヤ 3 マルチキャストを有効にします。

- a) レイヤ 3 マルチキャストを有効にする VRF を選択します。
- b) 右のプロパティサイドバーで、[L3 マルチキャスト (L3 Multicast)] チェックボックスをオンにします。

ステップ 5 1 つ以上のランデブー ポイント (RP) を追加します。

- a) VRF を選択します。
- b) 右のプロパティ サイドバーで、[ランデブー ポイントの追加 (Add Rendezvous Points)] をクリックします。
- c) VRF を選択したまま、右のサイドバーで [ランデブー ポイントの追加 (Add Rendezvous Points)] をクリックします。
- d) [ランデブー ポイントの追加 (Add Rendezvous Points)] ウィンドウで、RP の IP アドレスを入力します。
- e) RP のタイプを選択します。

- 静的 RP—RP が ACI ファブリックの外部にある場合。
- ファブリック RP—RP が ACI ファブリック内にある場合。

- f) (オプション) [マルチキャスト ルートマップ ポリシー (Multicast Route-Map Policy)] ドロップダウンから、以前に設定したルートマップ ポリシーを選択します。

デフォルトでは、入力した RP IP は、ファブリックのすべてのマルチキャスト グループに適用されます。RP を、特定のマルチキャスト グループのセットに制限する場合は、ルート マップ ポリシーでそれらのグループを定義し、ここでそのポリシーを選択します。

ステップ 6 L3Out で PIM を有効にします。

スタティック RP とファブリック RP の両方で、マルチキャストルーティングが有効になっている PIM 対応ボーダー リーフ スイッチが必要です。現在、L3Out 設定は Nexus Dashboard Orchestrator から実行できないため、サイトの APIC で PIM が有効になっていることを直接確認する必要があります。L3Out 上での PIM の設定の詳細については、[Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド](#)を参照してください。

- a) サイトの Cisco APIC にログインします。
- b) 上部のメニューで [テナント (Tenants)] をクリックし、L3Out を含むテナントを選択します。
- c) 左側のナビゲーションメニューで、[ネットワーキング (Networking)] > [L3Outs] > <l3out-name> を選択します。
- d) メイン ペインで、[ポリシー (Policy)] タブを選択します。
- e) [PIM] オプションを確認します。

Multi-Site は IPv4 マルチキャストのみをサポートします。

ステップ7 BD でレイヤ3 マルチキャストを有効にします。

いったん VRF で L3 マルチキャストを有効にすると、L3 マルチキャストをブリッジドメイン (BD) レベルで有効にすることができます。

- a) レイヤ3 マルチキャストを有効にする BD を選択します。
- b) 右のプロパティサイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ8 (オプション) マルチキャスト フィルタ処理を設定する場合は、送信元と接続先のフィルタ処理のためのルートマップを指定します。

- a) BD を選択します。
- b) 右のプロパティ サイドバーで、**[ルートマップの送信元フィルタ (Route-Map Source Filter)]** と **[ルートマップの接続先フィルタ (Route-Map Destination Filter)]** を選択します。

同じブリッジドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。

ルートマップを選択しなかった場合、デフォルトの動作は、「ブリッジドメインですべてのマルチトラフィックを許可する」になります。一方、ルートマップを選択すると、デフォルトの動作は、「ルートマップのフィルタエントリに明示的にマッチしないすべてのトラフィックを拒否」に変わることにご注意してください。

ステップ9 マルチキャスト ソースが1つのサイトにあり、他のサイトに拡張されていない場合は、EPG でサイト間マルチキャスト ソース オプションを有効にします。

BD で L3 マルチキャストを有効にしたら、マルチキャスト ソースが接続されている EPG (マルチキャスト 対応 BD の一部) でもマルチキャストを有効にする必要があります。

- a) レイヤ3 マルチキャストを有効にする EPG を選択します。
- b) 右のサイドバーで、**[サイト間マルチキャスト送信元 (Intersite Multicast Source)]** チェックボックスをオンにします。

ソース固有マルチキャスト (SSM) の有効化

以下の手順では、Nexus Dashboard Orchestrator GUI を使用して、VRF、BD、および EPG で SSM マルチキャストを有効にする方法を説明しています。ASM マルチキャストを有効にする場合は、代わりに [Any-Source Multicast \(ASM\) マルチキャストの有効化 \(272 ページ\)](#) の手順に従います。

始める前に

- [Layer 3 マルチキャストに関するガイドラインと制限事項 \(269 ページ\)](#) で説明されている情報を読んで、従っていることを確認してください。
- マルチキャストのフィルタリングを有効にする予定の場合には、[マルチキャストルートマップポリシーの作成 \(271 ページ\)](#) で説明されているように、必要なマルチキャストルートマップを作成します。

- サイトローカル レベルでマルチキャスト対応 BD の IGMPv3 インターフェイス ポリシーを設定する必要があることに注意してください。
- これについては、次の手順のステップ 8 で説明します。追加情報については、[Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド](#)を参照してください。

-
- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左側のサイドバーから、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] ビューを選択します。
- ステップ 3** 変更するスキーマをクリックします。
- ステップ 4** VRD でレイヤ 3 マルチキャストを有効にします。
- まず、サイト間で拡張されている VRF でレイヤ 3 マルチキャストを有効にします。
- a) レイヤ 3 マルチキャストを有効にする VRF を選択します。
 - b) 右のプロパティ サイドバーで、[L3 マルチキャスト (L3 Multicast)] チェックボックスをオンにします。
- ステップ 5** (任意) SSM リスナーのカスタム範囲を設定します。

デフォルトの SSM 範囲は 232.0.0.0/8 で、ファブリック内のスイッチで自動的に設定されます。SSM を使用している場合は、この範囲のグループに参加するようにリスナーを設定することを推奨します。この場合は、この手順をスキップできます。

何らかの理由でリスナー設定を変更しない場合は、最大 4 つの範囲を含むルートマップを作成して、VRF 設定で SSM 範囲を追加できます。新しい範囲を追加すると、その範囲が SSM 範囲になり、ASM に同時に使用できないことに注意してください。

カスタム SSM 範囲の設定は、サイトの APIC で直接行う必要があります。

- a) サイトの Cisco APIC にログインします。
- b) 上部のメニューで [テナント (Tenants)] をクリックし、VRF を含むテナントを選択します。
- c) 左側のナビゲーションメニューで、[ネットワーキング (Networking)] > [VRFs] > <VRF-name> > [マルチキャスト (Multicast)] を選択します。
- d) メイン ペインで、[パターン ポリシー (Pattern Policy)] タブを選択します。
- e) [ルート マップ (Route Map)] ドロップダウン ([ソース固有のマルチキャスト (Source Specific Multicast (SSM))] 領域) から、既存のルート マップを選択するか、[マルチキャストのためのルート マップ ポリシーの作成 (Create Route Map Policy for Multicast)] オプションをクリックして、新しいルート マップ ポリシーを作成します。

既存のルート マップを選択した場合は、ドロップダウンの横にあるアイコンをクリックして、ルート マップの詳細を表示します。

開いたルート マップの詳細ウィンドウまたは [マルチキャストのためのルート マップ ポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウで [+] をクリックしてエントリを追加します。次に、グループ IP を設定します。新しい範囲を定義するのに必要なのは、グループ IP アドレスだけです。

ステップ 6 (任意) サイトの L3Out で PIM を有効にします。

マルチキャストの送信元や受信者を外部ネットワーク ドメインに接続する場合は、サイトの L3Out でも PIM を有効にする必要があります。現在、L3Out 設定は Nexus Dashboard Orchestrator から実行できないため、サイトの APIC で PIM が有効になっていることを直接確認する必要があります。L3Out 上での PIM の設定の詳細については、[Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド](#)を参照してください。

- a) サイトの Cisco APIC にログインします。
- b) 上部のメニューで **[テナント (Tenants)]** をクリックし、L3Out を含むテナントを選択します。
- c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)] > [L3Outs] > <l3out-name>** を選択します。
- d) メイン ペインで、**[ポリシー (Policy)]** タブを選択します。
- e) **[PIM]** オプションを確認します。
Multi-Site は IPv4 マルチキャストのみをサポートします。

ステップ 7 BD でレイヤ 3 マルチキャストを有効にします。

いったん VRF で L3 マルチキャストを有効にすると、L3 マルチキャストをブリッジ ドメイン (BD) レベルで有効にすることができます。

- a) レイヤ 3 マルチキャストを有効にする BD を選択します。
- b) 右のプロパティ サイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 8 レシーバが接続されているブリッジ ドメインで IGMPv3 インターフェイス ポリシーを有効にします。

SSM を設定しているため、IGMPv3 インターフェイス ポリシーも BD に割り当てる必要があります。デフォルトでは、PIM がイネーブルの場合、IGMP も SVI で自動的にイネーブルになりますが、デフォルトバージョンは IGMPv2 に設定されます。IGMP インターフェイス ポリシーを明示的に IGMPv3 に設定する必要があります。これは、サイトローカル レベルで実行する必要があります。

- a) サイトの Cisco APIC にログインします。
- b) 上部のメニューで **[テナント (Tenants)]** をクリックし、BD を含むテナントを選択します。
- c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)] > [ブリッジ ドメイン (Bridge Domains)] > <BD-name>** を選択します。
- d) メイン ペインで、**[ポリシー (Policy)]** タブを選択します。
- e) **[IGMP ポリシー (IGMP Policy)]** ドロップダウンから IGMP ポリシーを選択するか、**[IGMP インターフェイス ポリシーの作成 (Create IGMP Interface Policy)]** をクリックして新しいポリシーを作成します。

既存のポリシーを選択した場合は、ドロップダウンの横にあるアイコンをクリックして、ポリシーの詳細を表示します。

開いているポリシーの詳細ウィンドウまたは**[マルチキャストのためのルート ポリシーの作成 (Create Route Map Policy for Multicast)]** ウィンドウで、**[バージョン (Version)]** フィールドが **[バージョン 3 (Version 3)]** に設定されていることを確認します。

ステップ 9 (オプション) マルチキャスト フィルタ処理を設定する場合は、送信元と接続先のフィルタ処理のためのルートマップを指定します。

- a) BD を選択します。
- b) 右のプロパティ サイドバーで、[ルートマップの送信元フィルタ (Route-Map Source Filter)] と [ルートマップの接続先フィルタ (Route-Map Destination Filter)] を選択します。

同じブリッジ ドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。

ルート マップを選択しなかった場合、デフォルトの動作は、「ブリッジ ドメインですべてのマルチキャストトラフィックを許可する」になります。一方、ルート マップを選択すると、デフォルトの動作は、「ルート マップのフィルタ エントリに明示的にマッチしないすべてのトラフィックを拒否」に変わることにご注意してください。

ステップ 10 マルチキャスト ソースが 1 つのサイトにあり、他のサイトに拡張されていない場合は、EPG でサイト間マルチキャスト ソース オプションを有効にします。

BD で L3 マルチキャストを有効にしたら、マルチキャスト ソースが接続されている EPG (マルチキャスト対応 BD の一部) でもマルチキャストを有効にする必要があります。

- a) レイヤ 3 マルチキャストを有効にする EPG を選択します。
- b) 右のサイドバーで、[サイト間マルチキャスト送信元 (Intersite Multicast Source)] チェックボックスをオンにします。



第 23 章

IPN 全体での QoS の保持

- [QoS およびグローバル DSCP ポリシー \(279 ページ\)](#)
- [DSCP ポリシーの注意事項と制限事項 \(279 ページ\)](#)
- [グローバル DSCP ポリシーの設定 \(280 ページ\)](#)
- [EPG およびコントラクトの QoS レベルの設定 \(282 ページ\)](#)

QoS およびグローバル DSCP ポリシー

Cisco ACI Quality of Service (QoS) 機能を使用すると、ファブリック内のネットワークトラフィックを分類し、トラフィックフローの優先順位付けとポリシングを行って、ネットワークの輻輳を回避できます。トラフィックがファブリック内で分類されると、QoS 優先度レベルが割り当てられます。この優先度レベルは、ネットワーク全体で最も望ましいパケットフローを実現するためにファブリック全体で使用されます。

Nexus Dashboard Orchestrator のこのリリースは、ソース EPG または特定のコントラクトに基づく QoS レベルの設定をサポートします。追加のオプションは、各ファブリックで直接使用できます。ACI QoS の詳細については、[Cisco APIC および QoS](#) を参照してください。

Cisco ACI ファブリック内でトラフィックが送受信される場合、QoS レベルは VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定されます。マルチポッドやリモートリーフトポロジなどの特定の使用例では、トラフィックはサイト間ネットワークを通過する必要があります。この場合、Cisco APIC の管理下でないデバイスはパケット内の CoS 値を変更できます。このような場合、パケット内の Cisco ACI QoS レベルと DSCP 値の間のマッピングを作成することで、同じファブリックまたは異なるファブリックの部分間で ACI QoS レベルを維持できます。

DSCP ポリシーの注意事項と制限事項

グローバル DSCP 変換ポリシーを設定する場合は、次の注意事項が適用されます。



(注) SD-WAN 統合とともにグローバル DSCP 変換ポリシーを使用する場合は、この章をスキップし、注意事項と制限事項の完全なリストを含むすべての情報について、[SD-WAN の統合 \(307 ページ\)](#) 章を参照してください。

- グローバル DSCP ポリシーは、オンプレミス サイトでのみサポートされます。
- グローバル DSCP ポリシーを定義する場合は、QoS レベルごとに一意の値を選択する必要があります。
- QoS レベルを割り当てる場合、特定のコントラクトまたは EPG 全体に割り当てることができます。

特定のトラフィックに複数の QoS レベルを適用できる場合は、次の優先順位を使用して 1 つだけが適用されます。

- コントラクト QoS レベル：コントラクトで QoS が有効になっている場合は、コントラクトで指定された QoS レベルが使用されます。
- 送信元 EPG QoS レベル：コントラクトに QoS レベルが指定されていない場合、送信元 EPG に設定された QoS レベルが使用されます。
- デフォルトの QoS レベル：QoS レベルが指定されていない場合、トラフィックにはデフォルトでレベル 3 の QoS クラスが割り当てられます。

グローバル DSCP ポリシーの設定

Cisco ACI ファブリック内でトラフィックが送受信される場合、VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定される ACI QoS レベルに基づいて優先順位が付けられます。マルチポッドおよびリモートリーフ トポロジなど、サイト間ネットワークに向けてトラフィックが ACI ファブリックを出ると、QoS レベルは VXLAN カプセル化パケットの外部ヘッダーに含まれる DSCP 値に変換されます。

ここでは、ACI ファブリックを出入りするトラフィックの DSCP 変換ポリシーを定義する方法について説明します。これは、トラフィックが非 ACI ネットワークを通過する必要がある場合に必要です。この場合、Cisco APIC の管理下でないデバイスは、通過するパケットの CoS 値を変更できます。

始める前に

- ACI ファブリック内の Quality of Service (QoS) 機能に精通している必要があります。QoS の詳細については、[Cisco APIC and QoS](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ2 グローバル DSCP ポリシー設定画面を開きます。

Multi-Site Orchestrator

Policies

Filter by attributes

Name	Type
Global DSCP Policy	cos-dscp

- [アプリケーション管理 (Application Management)] > [ポリシー (Policies)] の順に移動します。
- [グローバル DSCP ポリシー名 (Global DSCP Policy name)] をクリックします。

[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

ステップ3 グローバル DSCP ポリシーを更新します。

Edit Policy

Settings

User Level 1 Default SLA (43)	Control Plane Traffic AF12 medium drop
User Level 2 Voice-And-Video SLA (42)	Policy Plane Traffic AF33 high drop
User Level 3 Bulk-Data SLA (45)	SPAN Traffic AF31 low drop
User Level 4 2	Traceroute Traffic Expedited Forwarding
User Level 5 CS7	
User Level 6 AF13 high drop	

Associated Sites

Site	Translation Policy State
<input checked="" type="checkbox"/> Site1 4.2(2.66a)	<input checked="" type="checkbox"/> Enabled
<input checked="" type="checkbox"/> site2 4.2(3)	<input checked="" type="checkbox"/> Enabled

Save & Deploy

- a) 各 ACI QoS レベルの DSCP 値を選択します。
各ドロップダウンには、使用可能な DSCP 値のデフォルトリストが含まれています。レベルごとに一意の DSCP 値を選択する必要があります。
- b) ポリシーを展開するサイトを選択します。
エンドツーエンドの一貫した QoS 動作を実現するために、Multi-Site ドメインの一部であるすべてのサイトにポリシーを展開することを推奨します。
- c) 各サイトの展開時にポリシーを有効にするかどうかを選択します。
- d) [保存して展開 (Save & Deploy)] をクリックします。
保存して展開すると、DSCP ポリシー設定が各サイトにプッシュされます。設定を確認するには、サイトの APIC にログインし、[テナント (Tenants)] > [インフラ (infra)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L3 トラフィックの DSCP クラス CoS 変換ポリシー (DSCP class-CoS translation policy for L3 traffic)] に移動します。

次のタスク

グローバル DSCP ポリシーを定義したら、[EPG およびコントラクトの QoS レベルの設定 \(282 ページ\)](#) の説明に従って、ACI QoS レベルを EPG またはコントラクトに割り当てることができます。

EPG およびコントラクトの QoS レベルの設定

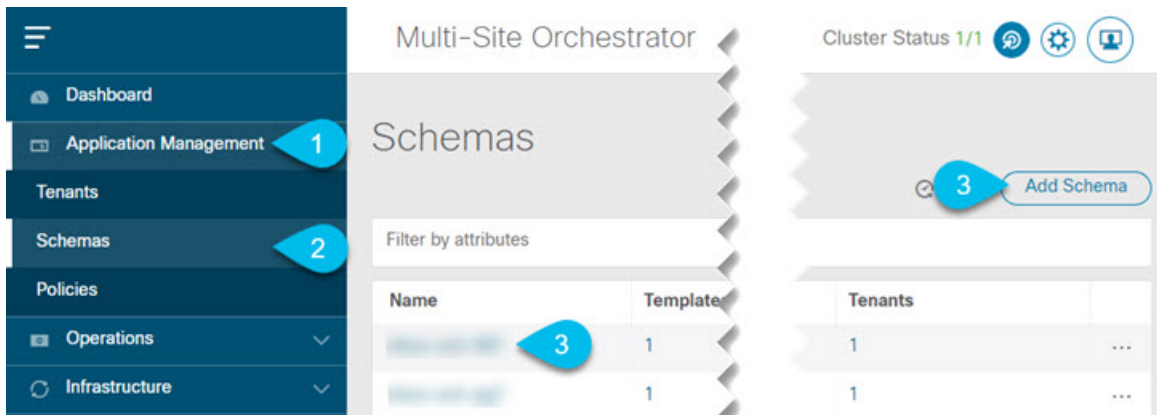
ここでは、ファブリック内のトラフィックの ACI QoS レベルを選択する方法について説明します。個々のコントラクトまたは EPG 全体に対して QoS を指定できます。

始める前に

- [グローバル DSCP ポリシーの設定 \(280 ページ\)](#) の説明に従って、グローバル DSCP ポリシーを定義しておく必要があります。
- ACI ファブリック内の Quality of Service (QoS) 機能に精通している必要があります。
QoS の詳細については、[Cisco APIC and QoS](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

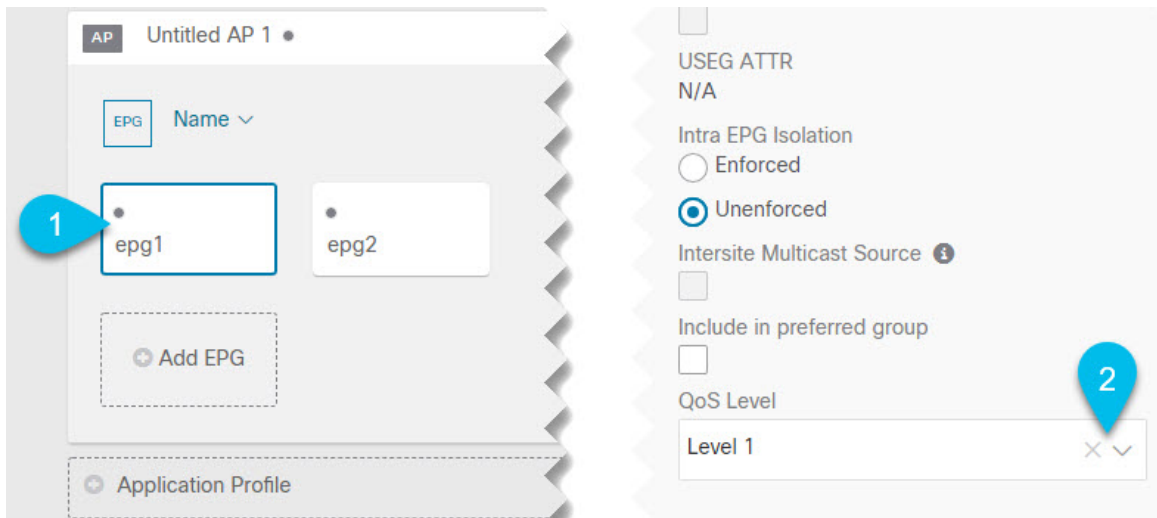
ステップ 2 編集するスキーマを選択します。



- [アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] > の順に移動します。
- 編集するスキーマの名前をクリックするか、[スキーマの追加 (Add Schema)] をクリックして新しいスキーマを作成します。

[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

ステップ3 EPG の QoS レベルの選択



- メインペインで、[EPG] エリアまでスクロールダウンして EPG を選択するか、[EPG の追加 (Add EPG)] をクリックして新しい EPG を作成します。
- 右側のサイドバーで [QoS レベル (QoS Level)] ドロップダウンまでスクロールし、EPG に割り当てる QoS レベルを選択します。

ステップ4 EPG の QoS レベルの選択

The screenshot displays the configuration interface for a Contract. On the left, the 'CONTRACT' section is visible, with a callout '1' pointing to the 'c1' contract name. Below it, the 'VRF' section shows 'vrf1'. On the right, the 'Filter Chain' section shows a table with one entry: 't1' with a 'Directive' of 'none'. Below this is a 'Service Graph' dropdown menu. A grey bar labeled 'ON-PREMISES PROPERTIES' is visible. Underneath, the 'QoS Level' dropdown menu is set to 'Level 1', with a callout '2' pointing to it.

Name	Directive
t1	none

ON-PREMISES PROPERTIES	
QoS Level	Level 1

- メインペインで、[コントラクト (Contract)] 領域までスクロールダウンしてコントラクトを選択するか、[+] アイコンをクリックして新しいコントラクトを作成します。
- 右側のサイドバーで、[QoS レベル (QoS Level)] ドロップダウンまでスクロールし、コントラクトに割り当てる QoS レベルを選択します。



第 24 章

SD-Access と ACI 統合

- Cisco SD-Access と Cisco ACI の統合 (285 ページ)
- マクロセグメンテーション (286 ページ)
- Cisco SD-Access および Cisco ACI 統合ガイドライン (289 ページ)
- DNA センターのオンボーディング (291 ページ)
- SD Access ドメインへの接続の構成 (291 ページ)
- SD Access to ACI 統合のステータスの表示 (293 ページ)
- 仮想ネットワークの拡張 (296 ページ)
- VN の VRF へのマッピングまたはマッピング解除 (298 ページ)
- トランジットルーティングの設定 (301 ページ)

Cisco SD-Access と Cisco ACI の統合



- (注) Cisco Nexus Dashboard と Cisco DNAC の統合により、Nexus とキャンパス SD Access ファブリックの展開全体で、ネットワーク接続のサブセットとマクロセグメンテーションシナリオの自動化が可能になります。この統合は、限られた可用性の下にあります。詳細についてはシスコの担当者にお問い合わせください。

Cisco Software-Defined Access (SD Access または SDA) は、Cisco Digital Network Architecture (DNA) 内のソリューションであり、Cisco の Intent-Based Networking (IBN) フレームワークを実装するキャンパスおよびブランチアーキテクチャを定義します。Cisco SD-Access は、セキュリティ、自動化、および保証によってビジネスニーズを満たす、統一されたポリシーベースの有線および無線ネットワークファブリックを定義します。Cisco Digital Network Architecture Controller (DNAC) は、Cisco Identity Services Engine (ISE) と組み合わせて、Cisco SD-Access ファブリックの自動化と管理の統合ポイントです。

Cisco Nexus Dashboard Orchestrator (NDO) のリリース 3.7(1) では、Cisco SD-Access および Cisco ACI 統合のサポートが追加されています。および ACI 統合の目的は、キャンパスおよびブランチネットワークをデータセンターネットワークに安全に接続することです。SD Access リリース 3.7(1) では、NDO は次の機能を実行できます。

- 両方のドメインからネットワークとリソースの情報を収集する
- ACI 側で VRF-Lite ドメイン間接続を自動的に設定する
- SD Access ボーダー ノードに接続されているネクスト ホップ デバイスの構成を提供します。
- クロスドメインの可視性を提供する

マクロセグメンテーション

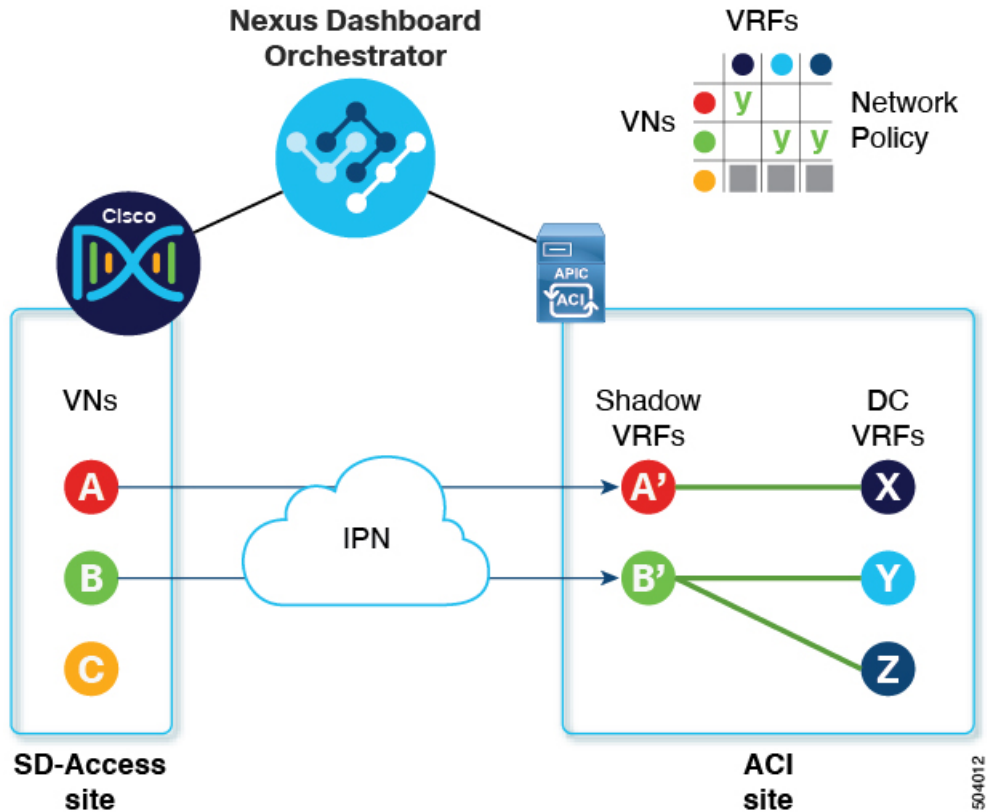
Cisco Nexus Dashboard Orchestrator (NDO) の Cisco SD-Access および Cisco ACI の統合機能により、ACI ドメインと SD Access ドメイン間のネットワーク要素のマクロセグメンテーションが可能になります。

ACI ドメインでは、EPG、サブネット、VLAN などのエンティティは、仮想ルーティングおよび転送インスタンス (VRF) の一部としてグループ化されます。VRF が外部通信を必要とする場合、VRF は ACI ボーダー リーフ (BL) の IP インターフェイス (L3Out) に関連付けられます。SD Access ドメインでは、ユーザー、サブネット、IP プールなどのエンティティを仮想ネットワーク (VN) としてグループ化できます。VN が外部通信を必要とする場合、VN は IP ハンドオフのために SD Access ボーダーノード (BN) インターフェイスに関連付けられます。2つのドメイン、ACI および SD Access のボーダー インターフェイスは、IP ネットワーク (IPN) を介して物理的に接続できますが、この基本的な接続は VRF と VN 間の接続を提供しません。Cisco Nexus ダッシュボード オーケストレーター Cisco SD-Access と Cisco ACI の統合により、管理者は、VRF を VN にマッピング (または「ステッチ」) するポリシーを作成できます。

マクロセグメンテーション ワークフロー

一般的な Cisco SD-Access と Cisco ACI の統合ワークフローは、次の図を参照する次の手順で構成されます。

図 28 : SD-Access-to-ACI 統合のための NDO を使用したマクロセグメンテーション



• 既存のサイトでは、Cisco Digital Network Architecture Controller (DNAC) 管理者がキャンパスファブリックを構成しており、一部のエンティティはデータセンターへのアクセスなどの外部アクセスを必要とします。SD AccessDNAC 管理者は、次のタスクを実行します。

- 作成済みの仮想ネットワーク (VN)
- それらの VN に関連付けられた IP アドレス プール
- 構成された L3 ボーダー ノードおよび関連するインターフェイス
- 作成済み IP (レイヤ 3) ハンドオフ トランジット ネットワーク
- 外部接続を必要とする VN 用に設定されたレイヤ 3 ハンドオフ

これらのタスクは通常の DNAC 管理タスクであり、Cisco SD-Access と Cisco ACI の統合のために特別な変更は加えられていないことに注意してください。

• NDO オペレーターは、DNAC ログイン情報を使用して、DNAC にログインして導入準備します。

オンボーディングプロセスでは、NDO は自動的に DNAC の REST API にアクセスして、サイト、VN、およびボーダーノードデバイスをクエリします。これらのエンティティを検出すると、NDO はどの VN が外部接続 (L3 ハンドオフ) 用に構成され、どの Cisco SD-Access ボーダーノードであるかを学習し、それらのサブネットを学習します。図 28 :

[SD-Access-to-ACI統合のためのNDOを使用したマクロセグメンテーション \(287ページ\)](#)
 に示す例では、VN A と B は L3 ハンドオフ用に設定されており、これらの VN は ACI サイトに拡張するために使用できます。VN C は L3 ハンドオフ用に構成されておらず、ACI サイトで使用できません。

NDO は、SD Access ファブリック内の進行中の構成変更について DNAC に定期的にクエリを実行し続けます。

- NDO オペレーターは、1 つ以上の ACI サイトと 1 つ以上の SD Access サイト間の接続を構成します。これには、ACI サイトのボーダーリーフスイッチとインターフェイス、およびボーダーリーフインターフェイスでの VRF-Lite 構成に使用される VLAN と IP プールの指定が含まれます。直接接続されたインターフェイス (IPN なし) の場合、VRF-Lite 構成は、SDA ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされた構成から取得され、VLAN と IP アドレスはこれらのプールから取得されません。

NDO は、拡張 SD Access VN のネクストホップデバイス構成を生成して表示します。この構成は、必要に応じて IPN デバイスに手動で適用できます。NDO は IPN デバイスをプロビジョニングしません。

- NDO オペレーターは VN をデータセンターに拡張し、VN を ACI ドメイン内の VRF に接続できるようにします。

VN を拡張すると、ACI ドメイン上の VN を表す VN の内部表現 (ミラーリングされた「シャドウ VRF」) が作成されます。図 1 の例では、シャドウ VRF A' と B' が ACI サイトに自動的に作成され、拡張 SD Access VN A と B を表します。これらのシャドウ VRF は、SD Access ドメインとの接続を必要とする ACI ドメイン内のすべてのサイトとポッドに拡張されます。NDO は、これらのシャドウ VRF が設定されているスキーマとテンプレートを自動的に作成します。自動作成されたスキーマとテンプレートは NDO に表示されますが、読み取り専用です。テンプレートは「共通」テナントに関連付けられており、「SDA 接続」が有効なすべてのサイトに関連付けられています。

- NDO オペレーターは、拡張 SD Access VN をデータセンター VRF または VN がアクセスする必要のある VRF にマッピングするネットワークポリシーを作成します。このアクションは、「VRF スティッチング」とも呼ばれます。データセンターの VRF は、さまざまな「アプリテナント」の一部にすることができます。これは、設計によるこの統合により、VRF 間接続 (通常は「共有サービス」と呼ばれる機能) を確立できることを意味します。

図 1 の例では、示されているネットワークポリシーは、拡張 SD Access VN A (VRF A' として拡張) をデータセンター VRF X に、VN B (VRF B' として拡張) をデータセンター VRF Y および Z にステッチしています。

このマッピングの結果として、すべてのトラフィックを許可するセキュリティポリシー関係が、拡張 SD Access VN に関連付けられた L3Out の外部 EPG とデータセンター VRF を表す vzAny 論理オブジェクトとの間に自動的に確立されます。この契約の適用により、拡張 SD Access VN のすべてのサブネットと、VRF 間で漏洩するように明示的に構成されたデータセンター VRF のすべてのサブネットとの間で無料の接続が可能になります。

Cisco SD-Access および Cisco ACI 統合ガイドライン

- ACI サイトと SD Access サイトは、外部 IP ネットワーク (IPN) を介して間接的に接続することも、ACI ボーダー リーフから SD Access ボーダー ノードへのバックツーバック接続で直接接続することもできます。
 - サイトが直接接続されている場合、2つのドメイン間の接続は、コントロールプレーンとデータプレーンの両方を含め、自動的に構成されます。
 - サイトが IPN を使用して接続されている場合、IPN デバイスは VRF Lite をサポートする必要があります。NDO および DNAC は IPN デバイスをプロビジョニングしませんが、NDO は、ACI ボーダー リーフおよび SD Access ボーダー ノードに直接接続されている IPN デバイスに適用できるサンプル設定を提供します。
- いずれかのドメインに複数のサイトが存在する場合は、次のガイドラインに注意してください。
 - SD Access サイトは別の SD Access サイト (SDA トランジット) を使用して ACI サイトに接続できます。
 - SD Access (キャンパス) ドメインに複数のサイトが存在する場合、各キャンパス サイトはデータセンター ドメインに直接接続するか (ダイレクト ピアリング)、汎用 IP ネットワーク (IPN) などの中間ネットワークを介して、または別のキャンパス サイトを介して (間接ピアリング) 接続できます。)。
 - ACI マルチサイト展開では、SD Access (キャンパス) ドメインとの直接または間接接続を必要とする各 ACI ファブリックは、ローカル L3Out 接続を展開する必要があります。ACI ファブリックがマルチポッドファブリックの場合、L3Out 接続は、同じファブリックの一部であるポッドまたはポッドのサブセットにのみ展開できます。
- [SD Access と ACI 統合のスケールビリティ \(290 ページ\)](#) で説明されている制限内で、VN から VRF への M:N マッピングがサポートされています。
- [SD Access と ACI 統合のスケールビリティ \(290 ページ\)](#) で説明されている制限内で、SD Access サイトから ACI サイトへの M:N マッピングがサポートされています。
- DNAC から、NDO はすべての SD Access (キャンパス) VN とそのサブネットについて学習します。VN が ACI サイトに拡張されると、NDO は、その拡張された VN のすべてのサブネットが ACI 境界リーフから到達可能であると想定します。NDO は、ACI ボーダー リーフにこれらのサブネットが存在するかどうかを定期的に確認します。拡張 VN の **[統合] > [DNAC] > [仮想ネットワーク]** テーブルの **[ステータス]** 列で、NDO はまだ到達できないサブネットを報告します。
- デフォルトでは、拡張 VN が DC VRF にマッピングされている場合、ACI サイトは通過ルートを VN にアドバタイズしません。NDO 管理者は、どの ACI サブネットが VN のシャドウ VRF にリークされるかを次のように制御します。

- ACI VRF の内部にある BD サブネットは、サブネットが「VRF 間で共有」で設定されている場合にのみリークされます。



(注) SD Access VN が複数の ACI VRF にマッピングされている場合、マッピングされたすべての ACI VRF で重複しないプレフィックスのみを「VRF 間で共有」として設定する必要があります。

- ACI VRF で設定された L3Out から学習した外部サブネットは、サブネットが「共有ルート制御」で設定されていて、トランジットルーティングが有効になっている場合にのみリークされます。

詳細については、[トランジットルーティングの設定 \(301 ページ\)](#) を参照してください。

- SD Access サイトは、ACI サイトへのインターネット接続を提供できません。
- IPv6 接続の自動化はサポートされていません。
- マルチキャストトラフィックはドメイン間でサポートされていません。

SD Access と ACI 統合のスケーラビリティ

- SD Access の NDO および ACI 統合にオンボーディングできる DNAC は 1 つだけです。
- 単一の DNAC で管理されている場合、複数の SD Access (キャンパス) サイトがサポートされます。
- SD Access のピアリングでは、最大 2 つの ACI サイトがサポートされます。各 ACI サイトは、単一のポッドファブリックまたはマルチポッドファブリックにすることができます。
- 仮想ネットワーク (VN) は、最大 10 個の ACI VRF にマッピングできます。
- SD Access ドメインから最大 32 個の仮想ネットワーク (VN) を ACI ドメインに拡張できます。

ソフトウェアの互換性

SD Access のマクロセグメンテーションと ACI 統合をサポートする最小ソフトウェアバージョンを次の表に示します。

製品	サポート対象の製品バージョン
NDO	3.7 以降のリリース
ACI	4.2 以降のリリース
DNAC	2.3.3 以降のリリース

DNA センターのオンボーディング

このセクションでは、Nexus Dashboard Orchestrator (NDO) を設定して DNA センター (DNAC) にログインする方法について説明します。ログイン後、NDO はドメインと ACI ドメイン間のネットワーク接続を作成するために必要なサイト構成情報をインポートできます。SD Access

ステップ 1 NDO にログインします。

ステップ 2 左側のナビゲーション ペインで、[インテグレーション (Integrations)] > [DNAC] を選択します。

ステップ 3 メイン ペインで、[DNAC の追加 (Add DNAC)] をクリックして DNA センターをオンボードします。

[DNAC の追加 (Add DNAC)] ダイアログボックスが開きます。

ステップ 4 [DNAC の追加 (Add DNAC)] ダイアログボックスで、次の手順を実行します。

- a) DNA センターの [名前 (Name)] を入力します。
- b) DNA センターの URL または IP アドレスをデバイス IP として入力します。
- c) DNA センターにログインするための [ユーザー名 (Username)] 資格情報を入力します。
読み取り専用アクセスで十分です。
- d) DNA センターにログインするための [パスワード (Password)] 資格情報を入力します。
- e) [Confirm Password (パスワードの確認)] に、もう一度パスワードを入力します。
- f) [Add] をクリックします。

NDO は、REST API を介して DNAC に自動的にログインし、DNAC によって制御されるドメイン内の仮想ネットワーク (VN) およびボーダーノード デバイスの構成を照会します。SD Access

次のタスク

- ACI サイトからサイトまたは IPN への接続を構成します。SD Access
- DNAC のドメインの VN と ACI ドメインの VRF 間の通信を許可するネットワーク ポリシーを作成します。SD Access

SD Access ドメインへの接続の構成

このセクションでは、ACI 統合のために Cisco SD-Access の NDO で実行されるインフラストラクチャ レベルの構成について説明します。ACI ファブリックごとに、Cisco SD-Access ドメインへの接続を提供する境界リーフ ノードとそれらに関連付けられたインターフェイスを選択する必要があります。

始める前に

DNA センターに登録している必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[インテグレーション (Integrations)] > [DNAC] を選択します。

ステップ 3 メイン ペインで、[概要 (Overview)] タブをクリックします。

DNA Center のダッシュボードが表示されます。

ステップ 4 [DNAC の詳細 (DNAC Details)] ボックスの右側で、[接続の構成 (Configuring Connectivity)] のリンクをクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 5 左側のナビゲーション ペインの [サイト] で、接続する ACI サイトを選択します。

[サイト接続] ウィンドウが右側に表示されます。

ステップ 6 [サイト接続] ウィンドウで、SDA 接続コントロールまで下にスクロールし、[有効] に設定します。

SDA 接続コントロールの下にいくつかのフィールドが表示されます。以下のサブステップで設定を構成します。

- a) [外部ルーテッドドメイン (External Routed Domain)] ドロップダウンリストから、接続する外部ルーテッドドメイン (L3 ドメイン) を選択します。

このルーテッドドメインは、APIC ですでに定義されている必要があります。

- b) [VLAN プール (VLAN Pool)] フィールドに、VLAN の番号の範囲を入力します。

このプールの VLAN 番号は、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。VLAN プールは、前の手順で選択した外部ルーテッドドメインに関連付けられた VLAN プールと同じか、そのサブセットである必要があります。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、VLAN ID はこのプールから割り当てられません。代わりに、VLAN ID は、SD Access ボードナーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

- c) [VRF Lite IP プール範囲 (VRF Lite IP Pool Ranges)] で、[VRF Lite IP プール範囲を追加 (Add VRF Lite IP Pool Range)] の横にある [+] 記号をクリックし、[IP アドレス (IP Address)] フィールドに IP サブネットを入力します。

このサブネットの IP アドレスは、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、これらのプールは使用されません。この場合、サブインターフェイスの IP アドレスは、SD Access ボードナーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

ステップ 7 ACI サイトのポッドが表示されている中央のペインで、SD Access サイトに接続するポッドの下にある [リーフノードの追加] をクリックします。

[**Select a Leaf** (リーフの選択)] ペインが右側に表示されます。以下のサブステップで設定を構成します。

- a) [**Select a Leaf** (リーフの選択)] ペインの [**リーフノード (Leaf Node)**] ドロップダウンリストから、SD Access ドメインに接続する境界リーフ スイッチを選択します。
- b) [**ルータ ID (Router ID)**] フィールドに、ボーダーリーフルータ ID を入力します。
- c) [**インターフェース**] で、[**インターフェースの追加**] の横にある + 記号をクリックします。

[Add Interface] ダイアログボックスが表示されます。

- d) [**インターフェイス ID (Interface ID)**] を入力します。
- e) [**インターフェイス タイプ (Interface Type)**] ドロップダウンリストから [**サブインターフェイス (Sub-Interface)**] または [**SVI**] を選択します。
- f) [**リモート自律システム番号 (Remote Autonomous System Number)**] を入力します。

SD Access 接続する ACI が IPN を使用する場合、この番号は IPN の ASN と一致する必要があります。

SD Access 接続への ACI が IPN なしでバックツーバックである場合、この番号は SD Access ボーダーノードの ASN と一致する必要があります。

- g) [保存 (Save)] をクリックします。

ステップ 8 [**ファブリック接続インフラ (Fabric Connectivity Infra)**] ページの上部のバーで、[**展開 (Deploy)**] をクリックします。

この時点では、設定はまだ APIC にプッシュされていません。最初の VN が拡張されると、SD Access 接続が自動的に構成されます。

SD Access to ACI 統合のステータスの表示

[**インテグレーション (Integrations)**] > [**DNAC**] メニューには、統合ステータスに関する詳細が表示され、使用可能な仮想ネットワーク (VN) のインベントリが提供されます。

[**概要 (Overview)**] タブ

[**概要 (Overview)**] タブは、次の情報ウィンドウを表示します。

- [**DNAC 詳細 (DNAC Details)**] : 接続されている DNAC の全体的なステータス、IP アドレス、およびバージョンを表示します。このウィンドウには、[**接続の構成 (Configure Connectivity)**] へのリンクも含まれています。
- 次のリソースの概要グラフィック ダッシュボード :
 - [**DNAC 可能なサイト (DNAC Enabled Sites)**] : DNAC によって管理されている SD Access サイトの数とタイプ。サポートされているサイトタイプは、オンプレミス、AWS、および DCNM です。
 - [**仮想ネットワーク (Virtual Networks)**] : 使用可能な VN の数、および拡張または拡張されていない数。

- **[DC VRF]** : 共有に使用できるデータセンター VRF の数、およびそれらがマッピングされているかどうか。

[仮想ネットワーク (Virtual Networks)] タブ

[仮想ネットワーク (Virtual Networks)] タブをクリックして、VN に関する詳細を表示します。

ページの上部のウィンドウには、**[概要 (Overview)]** タブからの概要グラフィック情報が繰り返されます。

このページの **[仮想ネットワーク (Virtual Networks)]** ウィンドウには、SD Access ボーダーノードでの IP ハンドオフ用に DNAC によって構成された仮想ネットワーク (VN) が一覧表示されます。VN のテーブルには、VN ごとに次の情報が表示されます。

- **[ステータス (Status)]** : VN の現在の統合ステータスと、ステータスの重大度を示す色分けされたアイコン。ステータスを次の表に示します。

ステータス	アイコンの色 (重大度)	説明
検出済	緑色 : 正常	VN は SDA ボーダー ノードで検出されます。
処理中	グレー (情報)	構成変更後の VN の最新ステータスの読み取り。これは一時的な状態です。 ヒント ページの右上隅にある [更新] アイコンをクリックして、ステータスの即時ポーリングを強制することができます。
成功	緑色 (正常)	VN は正常に拡張されました。
[BGPSessionIssues]	黄色 (警告)	すべてのインターフェイスで BGP セッションが確立されているわけではありません。詳細については、各 DC ボーダー リーフの状態を確認してください。
[RouteLeakPartial]	黄色 (警告)	VN サブネットは、DC ボーダー リーフ ノードに部分的に伝達されます。詳細については、各 DC ボーダー リーフの状態を確認してください。
[RouteLeakNone]	赤 (失敗)	VN サブネットはまだ DC 境界リーフ ノードに伝達されていません。VN テーブルで [DC サイト (DC Sites)] をクリックして、DC ボーダー リーフ インターフェイスに問題がないか確認します。
[MapVRFConfigFailure]	赤 (失敗)	マッピングされた VRF で設定が失敗しました。マッピングを再実行します。
[DCSiteConfigFailure]	赤 (失敗)	DC サイトで VN 拡張が失敗しました。VN の拡張を解除して、再度拡張します。

VNのステータスアイコンをクリックして、警告やエラーのトラブルシューティングに役立つ追加の詳細を含むサイドバーを表示します。

- **[名前 (Name)]** : DNAC 管理者によって VN に割り当てられた名前。
- **[拡張済み (Extended)]** : VN が拡張されているかどうかを示します。
- **[DC マップされた VRF (DC Mapped VRFs)]** : VN がマップされるデータセンター VRF の数。この番号をクリックしてサイドバーを開き、マッピングされたデータセンター VRF の関連スキーマ、テンプレート、およびテナントを表示します。
- **[DC サイト (DC Sites)]** : VN がマップされているデータセンター サイトの数。この番号をクリックしてサイドバーを開き、ボーダー リーフ インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、データセンター サイトの詳細を表示します。



ヒント IPN接続のボーダーリーフインターフェイスの場合、サイドバーの[ピアデバイスの構成 (Peer Device Configuration)]で、[詳細の表示 (Show Details)]をクリックして、このサイトに接続されている IPN デバイスの構成例を表示します。

- **[キャンパス サイト (Campus Sites)]** : この VN に関連付けられているキャンパス サイトの数。この番号をクリックしてサイドバーを開き、ボーダー ノード インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、キャンパス サイトの詳細を表示します。



ヒント IPN接続ボーダーノードインターフェイスの場合、サイドバーの[ピアデバイス構成]の下にある[詳細を表示]をクリックして、このサイトに接続されている IPN デバイスのサンプル構成を表示します。

- **[... (アクション アイコン) (... (actions icon))]** : アイコンをクリックして、この VN のアクションにアクセスします。

使用可能なアクションは、VN の現在のステータスによって異なりますが、次のものが含まれる場合があります。

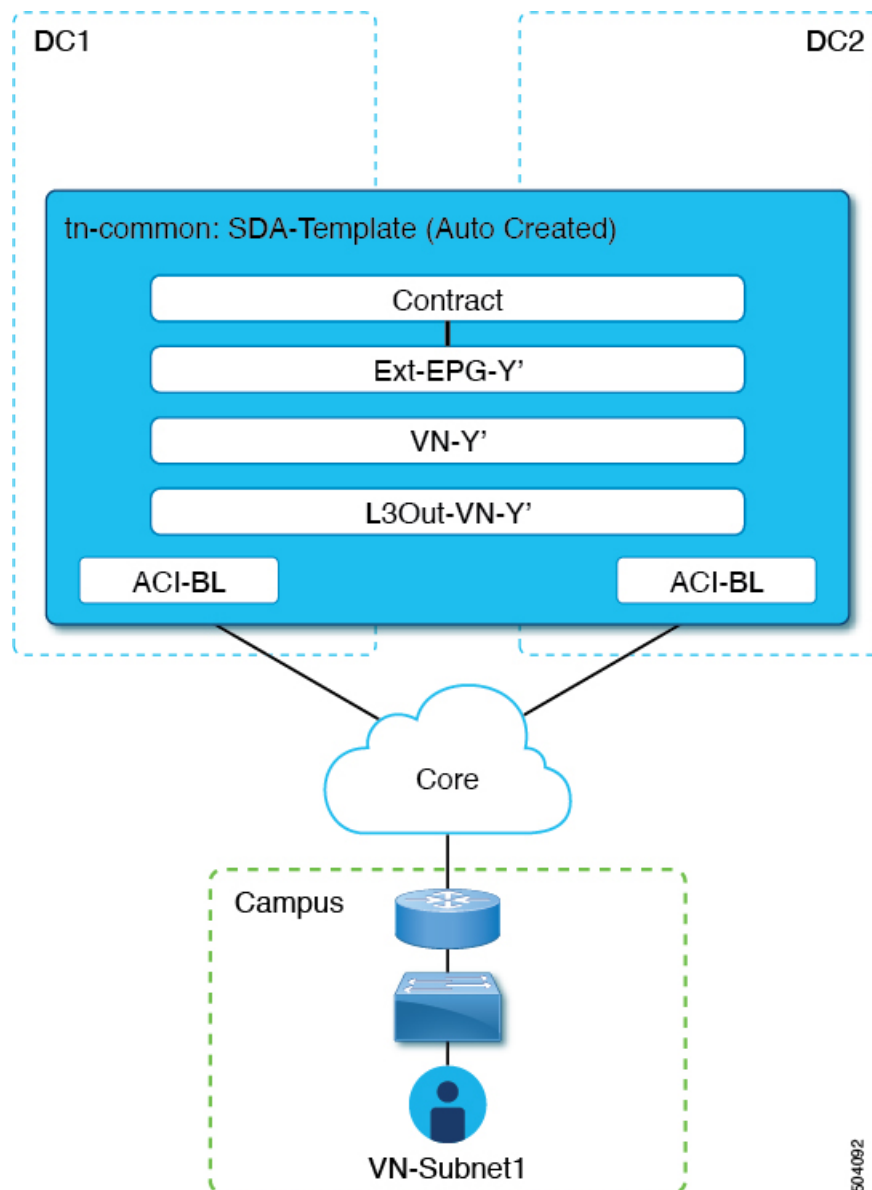
- VN の拡張 / 拡張解除
- DC VRF のマッピング / マッピング解除
- トランジット ルートの有効化 / 無効化

キャンパス VN をデータセンター VRF にマッピングすると、[仮想ネットワーク (Virtual Networks)] ページの [関連付けテンプレート (Associated Templates)] ウィンドウが表示されます。

仮想ネットワークの拡張

このセクションでは、SD Access (キャンパス) VN を ACI (データセンター) ファブリックに拡張する方法について説明します。このアクションにより、DC 側のキャンパス VN のミラーリングされたイメージを表す VRF (および [図 29: VN の拡張 \(296 ページ\)](#) に示す他の関連する設定オブジェクト) が作成されます。作成されたオブジェクトは、「共通」テナントに関連付けられた自動生成テンプレートで定義されます。

図 29: VN の拡張



504092

始める前に

- DNA センター (DNAC) をオンボーディングしておく必要があります。
- ACI サイト レベルでSD Accessドメインへの接続を構成しておく必要があります。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[インテグレーション (Integrations)] > [DNAC] を選択します。

ステップ 3 メイン ペインで、[仮想ネットワーク (Virtual Networks)] タブをクリックします。

仮想ネットワーク (VN) のテーブルが表示され、SD Access ボーダー ノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。

ステップ 4 拡張する VN の行で、アクションメニュー ([...]) をクリックし、[拡張 (Extend)] を選択します。

ダイアログ ボックスが開き、VN が拡張される ACI サイトとインターフェイスが表示されます。この情報は、[SD Accessドメインへの接続の構成 \(291 ページ\)](#) の構成設定を反映しています。

VNの拡張を後で取り消す場合は、アクションメニュー ([...]) をクリックし、[拡張解除 (Unextend)] を選択します。

ステップ 5 ダイアログボックスで、[はい (Yes)] をクリックします。

VN は、SD Access 接続が有効になっているすべての ACI サイトに拡張されますが、まだどの ACI VRF にもマッピングされていません。

ステップ 6

次のタスク

ACI ボーダー リーフ インターフェイスの BGP ピアリング ステータスを確認します。

- SD Access ボーダーノードと ACI ボーダー リーフが直接 (バックツーバック) 接続されている場合は、キャンパスVNを拡張した結果として、これらのデバイス間でBGPセッションが確立されていることを確認します。[インテグレーション (Integrations)] > [DNAC] > [仮想ネットワーク (Virtual Networks)] で、[DC サイト (DC Sites)] 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ インターフェイスの詳細を表示します。ボーダー リーフ インターフェイスの BGP Peering Status が「Up」を示していることを確認します。
- IPNがドメイン間に展開されている場合は、構成サンプルを取得して、ボーダーノードおよびACI ボーダー リーフに直接接続されているネクストホップデバイスの構成を支援します。SD Access[インテグレーション (Integrations)] > [DNAC] > [仮想ネットワーク (Virtual Networks)] で、[DC サイト (DC Sites)] 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ インターフェイスの詳細を表示します。IPN接続された境界リーフ インターフェイスの場合は、[ピアリング デバイス構成] の横にある [詳細を表示] リンクをクリックして、サンプルの IPN デバイス構成を表示します。IPN デバイスを設定した

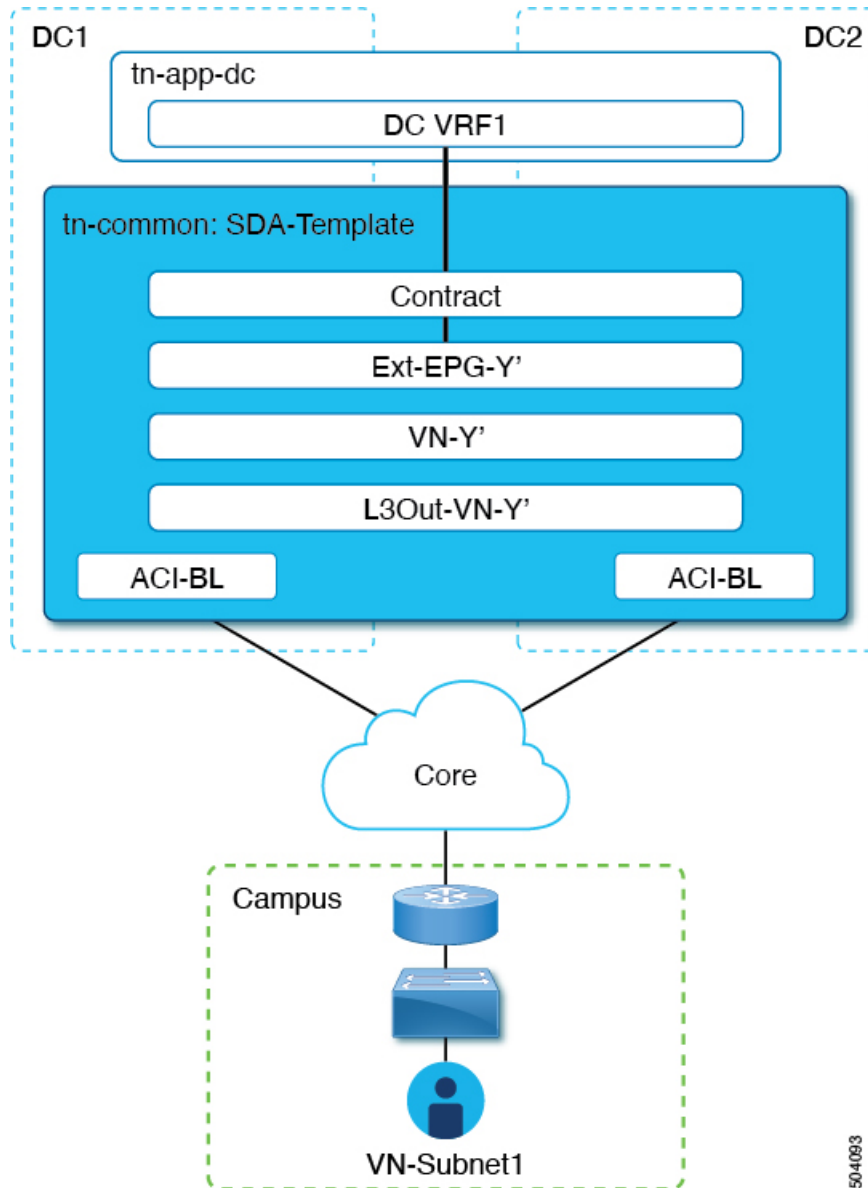
ら、境界リーフ インターフェイスの BGP ピアリング ステータスが「アップ」を示していることを確認します。

[VN の VRF へのマッピングまたはマッピング解除 \(298 ページ\)](#) で説明されているように、拡張 VN を 1 つ以上の ACI VRF にマッピングします。

VN の VRF へのマッピングまたはマッピング解除

このセクションでは、仮想ネットワーク (VN) を ACI ファブリック内の 1 つ以上のデータセンター (DC) VRF にマッピング (「ステッチ」) する方法について説明します。[図 30 : VRF へのマッピング \(299 ページ\)](#) に示すように、VRF へのマッピングにより、DCVRF (「vzAny」オブジェクトによって表される) と「共通」テナントで以前にプロビジョニングされた外部 EPG との間の契約関係が確立されます。

図 30: VRF へのマッピング



始める前に

VN を ACI サイトに拡張しておく必要があります。

-
- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
 - ステップ 2 左側のナビゲーション ペインで、[インテグレーション (Integrations)] > [DNAC] を選択します。
 - ステップ 3 メイン ペインで、[仮想ネットワーク (Virtual Networks)] タブをクリックします。

仮想ネットワーク (VN) のテーブルが表示され、SD Access ボーダー ノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。

- ステップ 4** マッピングする VN の行で、アクションメニュー ([...]) をクリックし、**[DC VRF のマッピング / マッピング解除 (Map/Un-Map DC VRFs)]** を選択します。
- [DC VRF のマップ/マップ解除 (Map/Un-Map DC VRFs)]** ダイアログ ボックスが開きます。
- ステップ 5** **[DC VRF のマップ / マップ解除 (Map/Un-Map DC VRFs)]** ダイアログボックスで、**[DC VRF のマップの追加 (Add Mapped DC VRF)]** の横にある **[+]** アイコンをクリックします。
- ステップ 6** VRF のドロップダウンリストから VRF を選択します。
- 選択した VRF がテーブルに追加され、VRF のテンプレートも表示されます。後の手順で必要になるため、テンプレート名を書き留めておいてください。
- VN を追加の VRF にマッピングする場合は、**+** アイコンを再度クリックして、ドロップダウンリストから追加の VRF を選択します。
- 既存のマッピングを削除して、DC VRF のマッピングを解除することもできます。DC VRF のマッピングを解除するには、VRF の行にあるごみ箱アイコンをクリックします。
- ステップ 7** **[保存]** をクリックし、VN ステータスが **[成功]** に変わるまで待ちます。
- (注) この時点で、VN ステータスが「成功」を示していても、拡張 VN と DC VRF 間のデータ接続はまだ確立されていません。マッピング操作により、マッピングされた VRF に関連付けられたテンプレートが変更されました。接続が確立される前に、テンプレートを再展開する必要があります。VN テーブルの下の **[関連付けられたテンプレート (Associated Templates)]** テーブルに、マッピングされた VRF に関連付けられたテンプレートが表示されます。
- ステップ 8** **[インテグレーション (Integrations)] > [DNAC] > [仮想ネットワーク (Virtual Networks)]** タブの **[関連付けられたテンプレート (Associated Templates)]** テーブルで、マッピングされた VRF に関連付けられたテンプレートのリンクをクリックします。
- スキーマとテンプレート ページが開きます。
- ステップ 9** スキーマとテンプレートのページで、**[サイトに配置 (Deploy to sites)]** をクリックします。
- ステップ 10** テンプレートのレビューと承認 (変更管理) が有効になっている場合は、変更管理ワークフローに従ってテンプレートを再展開します。それ以外の場合、**[展開 (Deploy)]** をクリックして、テンプレートを再展開します。

次のタスク



- (注) DC VRF のマッピングを解除した場合、**[関連付けられたテンプレート (Associated Templates)]** テーブルにテンプレートは表示されません。ただし、**[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)]** に移動して、関連付けられたテンプレートを再展開して、vzAny 構成を削除する必要があります。それ以外の場合、データプレーン通信は有効のままです。

トランジットルーティングの設定

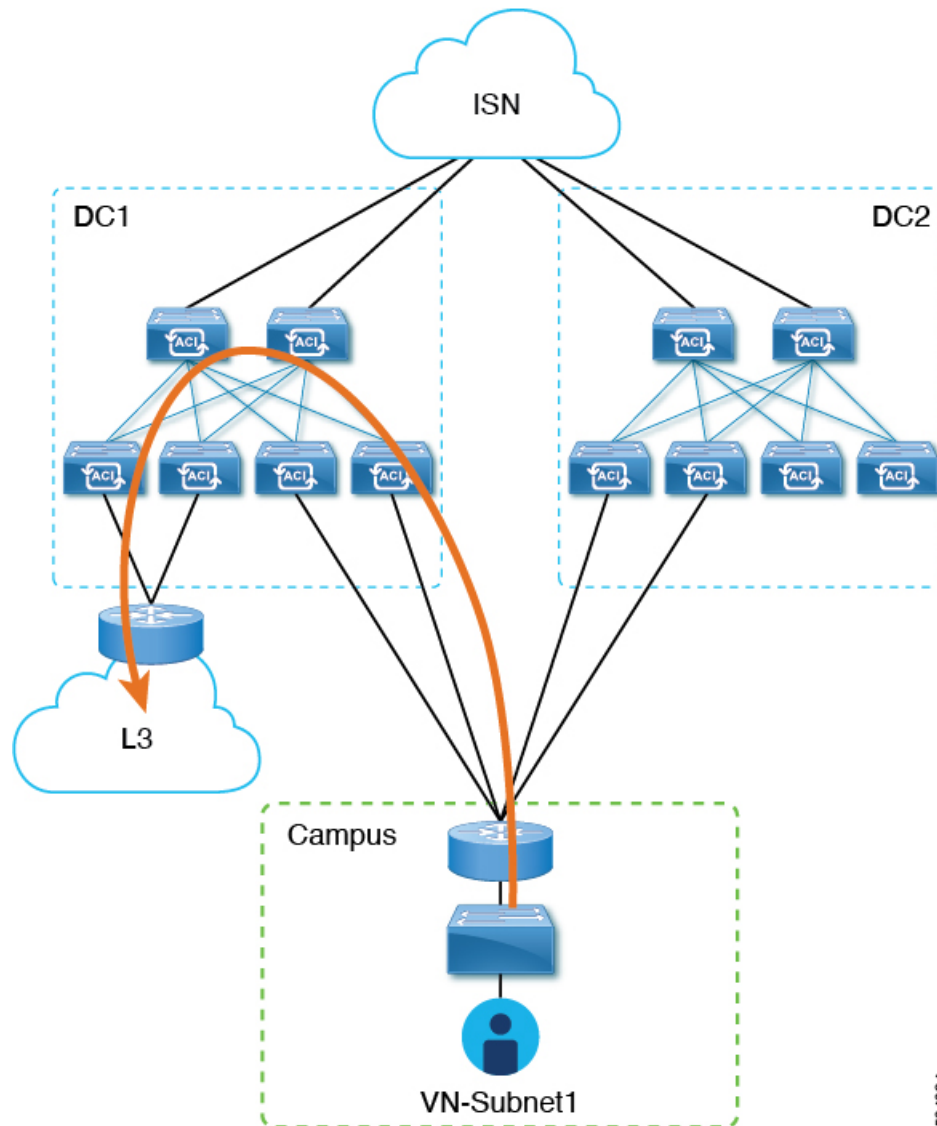
拡張 SD Access (キャンパス) VN が ACI (データセンター) VRF にマッピングされると、「外部でアドバタイズされる」フラグと「VRF 間で共有される」フラグが設定されている DC VRF の BD サブネットは、「共通」テナント VRF にリークされ、その後 SD Access ドメインに向けてアドバタイズされます。これにより、キャンパス ユーザーは DC VRF でプロビジョニングされたアプリケーションにアクセスできるようになります。



-
- (注) SD Access VN が複数の ACI VRF にマッピングされている場合、マッピングされたすべての ACI VRF で重複しないプレフィックスのみを「VRF 間で共有」として設定する必要があります。
-

これらの BD サブネットのアドバタイズに加えて、キャンパス ユーザーが ACI ドメインをトランジットとして使用して外部 L3 ネットワーク ドメインにアクセスする必要がある場合があります ([図 31: トランジットとしての ACI ドメイン \(302 ページ\)](#))。

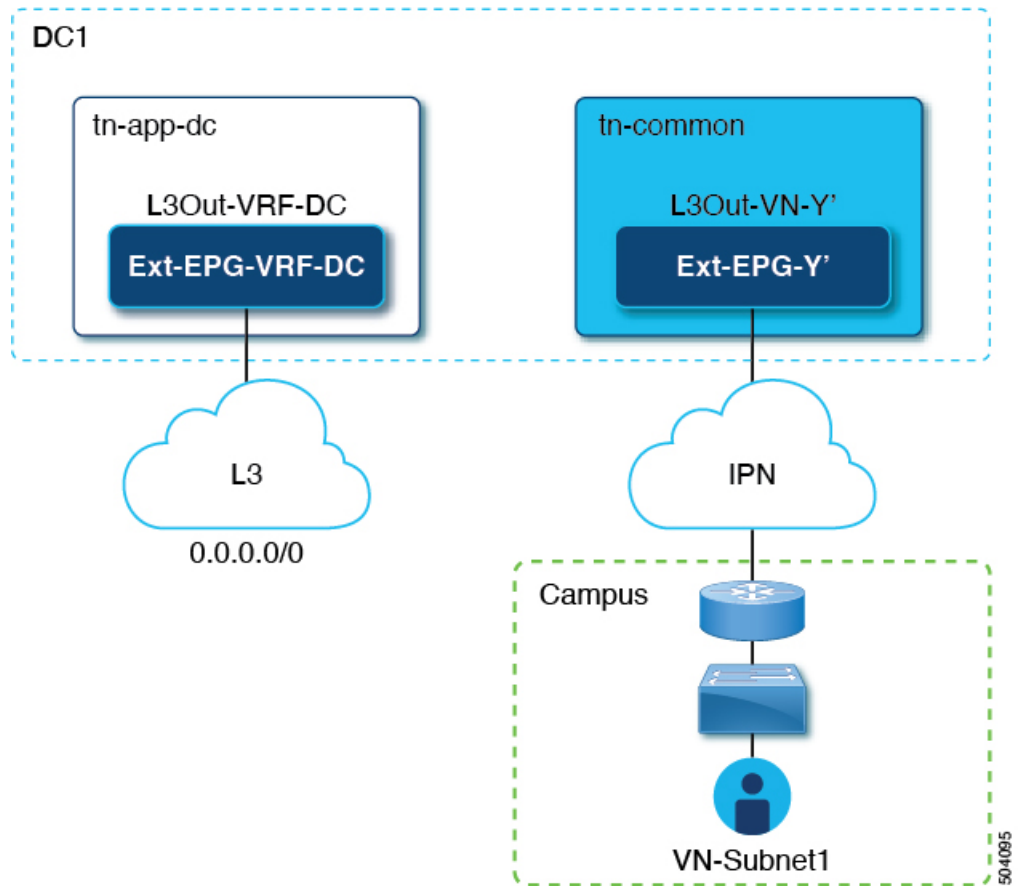
図 31: トランジットとしての ACI ドメイン



50-4094

このシナリオでは、DC VRF (L3Out-DC-VRF) に関連付けられた L3Out 接続は、通常、外部ドメインへの接続を許可するためにプロビジョニングされ、外部ルート (図 32 : L3Out 接続 (303 ページ) の例では単純な 0.0.0.0/0 デフォルト) が DC VRF ルーティングテーブル (tn-app-dc の一部) にインポートされます。

図 32: L3Out 接続



キャンパスユーザーがデータセンター経由で外部 L3 ドメインに接続できるようにするには、外部ルートを tn-common VRF にリークして、DC へのキャンパス VN 拡張の結果として自動生成された L3Out 接続 (L3Out-VN-Y') を介してキャンパス ドメインに向けてアドバタイズできるようにする必要があります。

外部ルートのリークを有効にするには、次の手順に従います。

始める前に

拡張キャンパス VN をデータセンター VRF にマッピングし、接続を確立しておく必要があります。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左側のナビゲーション ペインで、[インテグレーション (Integrations)] > [DNAC] を選択します。
- ステップ 3 メイン ペインで、[仮想ネットワーク (Virtual Networks)] タブをクリックします。
- ステップ 4 マッピングに成功したキャンパス VN の行で、アクションメニュー (...) をクリックし、[トランジットルーティングを有効にする] を選択します。

この構成(図 33: エクスポート ルート制御 (304 ページ))は、Ext-EPG-Y'の下に0.0.0.0/0プレフィックスを作成し、次の「ルート制御」フラグを設定して、tn-app-dc テナントからリークされたすべての外部ルートのIPN へのアドバタイジングを許可します。

図 33: エクスポート ルート制御

Update Subnet 0.0.0.0/0

Subnet *
0.0.0.0/0

Route Control Aggregate

Export Route Control Aggregate Export

Import Route Control

Shared Route Control

External EPG Classification

External Subnets for External EPG

Shared Security Import

トランジットルーティングを無効にするには、アクションメニュー ([...]) をクリックし、[トランジットルートを無効にする (Disable Transit Route)] を選択します。

(注) いずれかの設定 (有効または無効) で、キャンパス サイトは ACI VRF 内部の共有 BD サブネットにアクセスできます。

- ステップ 5** 左側のナビゲーション ペインから、[アプリケーション管理] > [スキーマ] を選択し、データセンター テナント アプリケーションを構成するためのテンプレートに移動します。
- ステップ 6** データセンター テナント アプリケーション テンプレートで、DC VRF の Ext-EPG-VRF-DC に関連付けられた 0.0.0.0/0 プレフィックスの下にフラグを設定して、インターネットから学習した外部ルートを tn-common にリークできるようにします (図 34: 共有ルート コントロール (304 ページ))。

図 34: 共有ルート コントロール

Update Subnet 0.0.0.0/0

Subnet *
0.0.0.0/0

Route Control Aggregate

Export Route Control

Import Route Control

Shared Route Control Aggregate Shared Routes

External EPG Classification

External Subnets for External EPG

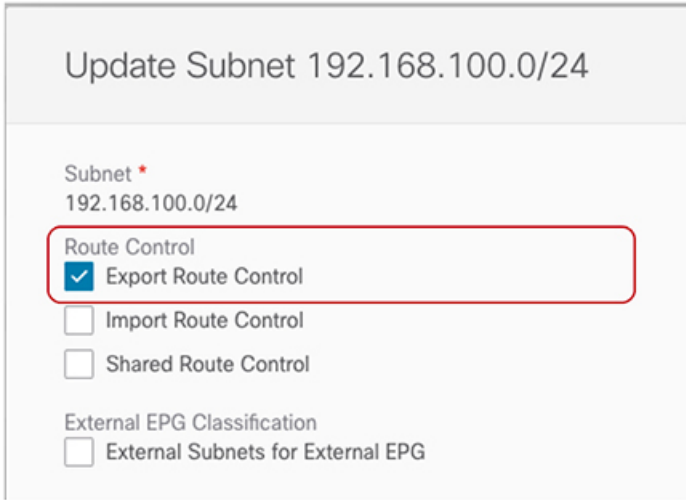
Shared Security Import

(注) 示されている設定により、L3Out-VRF-DCで受信されたすべての外部プレフィックスがtn-commonにリークされるため、キャンパスドメインに向けてアドバタイズされます。この設定により、L3ドメインから受信した場合、0.0.0.0/0デフォルトルートへのリークも許可されます。必要に応じて、外部プレフィックスのサブセットのみをtn-commonにリークできる、より詳細な構成を適用できます。これは、プレフィックスのこれらのサブセットに一致する特定のエントリーを作成し、それらのエントリーに「ここに」示されているのと同じフラグ構成を適用することによって実現されます。

ステップ 7 データセンターテナントアプリケーションテンプレートで、外部L3ドメインに向けてアドバタイズされるキャンパスVNサブネット（またはサブネットのセット）に一致するExt-EPG-VRF-DCの下に特定のプレフィックスを定義します。

に示す例では、この設定は特定の192.168.100.0/24プレフィックスに適用されます。[図 35: サブネットの更新 \(305 ページ\)](#)

図 35: サブネットの更新



Update Subnet 192.168.100.0/24

Subnet *
192.168.100.0/24

Route Control

- Export Route Control
- Import Route Control
- Shared Route Control

External EPG Classification

- External Subnets for External EPG

(注) VNサブネットに個別のプレフィックスを作成すると、外部L3ドメインへのキャンパスVNサブネットのアドバタイズを最も詳細なレベルで制御できます。このような細かい制御が必要ない場合は、代わりに0.0.0.0/0プレフィックスに関連付けられた「ルート制御のエクスポート」フラグを設定できます。これにより、tn-commonからtn-app-dcに漏えいしたすべてのキャンパスVNサブネットを外部ドメインに送信できます。



第 25 章

SD-WAN の統合

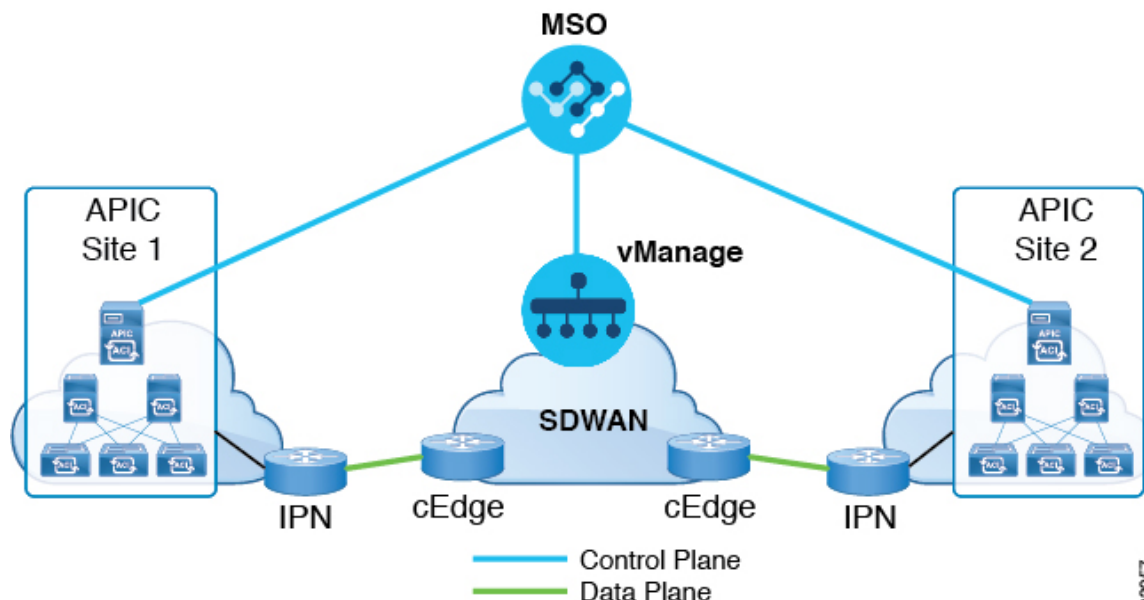
- [SD-WAN の統合 \(307 ページ\)](#)
- [SD-WAN 統合の注意事項と制約事項 \(308 ページ\)](#)
- [vManage コントローラの追加 \(309 ページ\)](#)
- [グローバル DSCP ポリシーの設定 \(310 ページ\)](#)
- [EPG およびコントラクトの QoS レベルの設定 \(312 ページ\)](#)

SD-WAN の統合

Cisco ソフトウェア定義ワイドエリア ネットワーク (SD-WAN) は、クラウド提供型のオーバーレイ WAN アーキテクチャです。単一のファブリックにより、ブランチをデータセンターとマルチクラウド環境に接続できるのが特長です。Cisco SD-WAN は、アプリケーションの予測可能なユーザエクスペリエンスを保証し、SaaS、IaaS、および PaaS 接続を最適化し、オンプレミスまたはクラウドで統合セキュリティを提供します。分析機能による可視化とインサイトは、問題を切り分けて迅速に解決するために役立ちます。プランニングと what-if シナリオ分析に欠かせない、高度なデータ解析も提供します。

データプレーン側では、SD-WAN は ASR または ISR ルータをエッジデバイスとして展開し (次の図では cEdge として表示)、各ファブリックのスパイン スイッチはこれらのエッジデバイスに接続します。SD-WAN は vManage と呼ばれる別のコントローラによって管理されます。これにより、サービスレベル契約 (SLA) ポリシーを定義して、DSCP 値に基づいて SD-WAN 内の各パケットのパスを選択する方法を決定できます。

図 36: Multi-Site と SD-WAN の統合



503057

Cisco Nexus Dashboard Orchestrator のリリース 3.0(2) では、SD-WAN 統合のサポートが追加されています。vManage コントローラから SLA ポリシーをインポートし、各 SLA ポリシーに DSCP 値を割り当て、vManage コントローラに DSCP から SLA へのマッピングを通知するように NDO を設定できます。これにより、事前設定された SLA ポリシーを適用して、SD-WAN 上のサイト間トラフィックのバケット損失、ジッター、および遅延のレベルを指定できます。SD-WAN 機能を提供する外部デバイスマネージャとして設定されている vManage コントローラは、SLA ポリシーで指定された損失、ジッター、および遅延パラメータを満たす最適な WAN リンクを選択します。

マルチサイト SD-WAN の統合により、複数のファブリック間のトラフィックが SD-WAN ネットワークを通過できるようになり、リモートサイトからのリターントラフィックが割り当てられた ACI QoS レベルを維持できるようになります。Cisco NDO を vManage に登録すると、SLA ポリシーがインポートされ、ACI QoS レベルを適切な DSCP 値に変換できます。NDO は、SD-WAN を通過するトラフィックに DSCP 変換ポリシーを適用して、リターントラフィックで Quality of Service を有効にします。

リリース 3.0(2) では、NDO GUI で契約および EPG に直接 ACI QoS レベルを割り当てることもできます。トラフィックがファブリックを離れるたびに、その QoS レベルが DSCP 値に変換され、vManage が SD-WAN 経由のトラフィックのパスを選択するために使用されます。

SD-WAN 統合の注意事項と制約事項

Multi-Site と SD-WAN の統合を有効にする場合は、次のガイドラインが適用されます。

- サイト間の east-west トラフィックに対して均一なユーザー QoS レベルと DSCP 変換を有効にするには、各ファブリックのスパインスイッチを直接または複数のホップを介して SD-WAN エッジ デバイスに接続する必要があります。

これは、リーフスイッチを SD-WAN エッジデバイスに接続する必要がある north-south トラフィックの APIC SD-WAN 統合の既存の実装とは対照的です。

- グローバル DSCP ポリシーは、オンプレミス サイトでのみサポートされます。
- SD-WAN 統合は、Cisco Application Services Engine の Nexus Dashboard Orchestrator 展開でのみサポートされます。

詳細については、[Deployment Overview](#)の章（*Cisco Nexus Dashboard Orchestrator Installation and Upgrade Guide*）を参照してください。

- グローバル DSCP ポリシーを定義する場合は、QoS レベルごとに一意の値を選択する必要があります。
- 既存の DSCP ポリシー値に加えて、vManage から最大 4 つの SLA ポリシーをインポートできます。値は、41、42、43、45、47、49のいずれかです。
- SLA ポリシーは、Cisco vManage ですでに定義されている必要があります。
- QoS レベルを割り当てる場合、特定のコントラクトまたは EPG 全体に割り当てることができます。

特定のトラフィックに複数の QoS レベルを適用できる場合は、次の優先順位を使用して 1 つだけが適用されます。

- コントラクト QoS レベル：コントラクトで QoS が有効になっている場合は、コントラクトで指定された QoS レベルが使用されます。
- 送信元 EPG QoS レベル：コントラクトに QoS レベルが指定されていない場合、送信元 EPG に設定された QoS レベルが使用されます。
- デフォルトの QoS レベル：QoS レベルが指定されていない場合、トラフィックにはデフォルトでレベル 3 の QoS クラスが割り当てられます。

vManage コントローラの追加

このセクションでは、vManage コントローラを Nexus Dashboard Orchestrator に追加して、設定済みの SLA ポリシーをインポートする方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 vManage コントローラを追加します。

- a) [インテグレーション (Integration)] > [SD-WAN] に移動します。
- b) [ドメイン コントローラの追加 (Add Domain Controller)] をクリックします。

[ドメインの追加 (Add Domain)] ウィンドウが開きます。

ステップ 3 vManage コントローラ情報を入力します。

表示された [エントリの追加 (Add Entry)] ウィンドウで、次の情報を入力します。

- NDO に表示する vManage ドメインの名前。
- デバイスの IP アドレスまたは完全修飾ドメイン名 (FQDN)。
- vManage コントローラへのログインで使用するユーザ名とパスワード。

[追加 (Add)] をクリックして vManage ドメインを保存します。vManage コントローラの情報を入力した後、既存の SLA ポリシーのリストがメイン ペインに表示されるまでに最大 1 分かかります。

次のタスク

[グローバル DSCP ポリシーの設定 \(310 ページ\)](#) の説明に従って、Nexus Dashboard Orchestrator でグローバル DSCP ポリシーを定義します。

グローバル DSCP ポリシーの設定

Cisco ACI ファブリック内でトラフィックが送受信される場合、VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定される ACI QoS レベルに基づいて優先順位が付けられます。トラフィックがスパインスイッチからサイト間ネットワークへの ACI ファブリックを出ると、QoS レベルは VXLAN カプセル化パケットの外部ヘッダーに含まれる DSCP 値に変換されます。

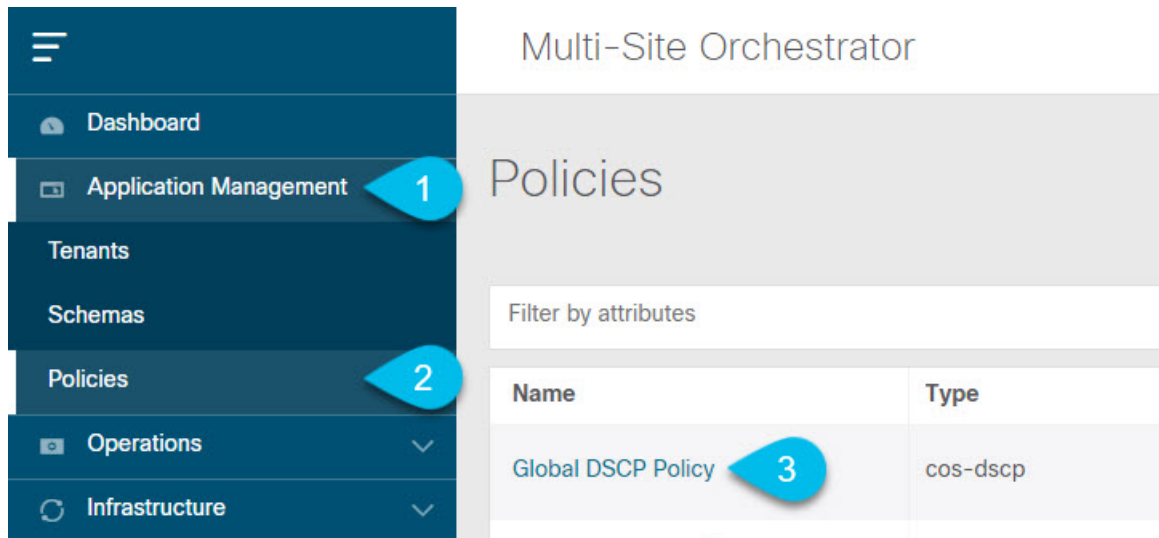
ここでは、ACI ファブリックを出入りするトラフィックの DSCP 変換ポリシーを定義する方法について説明します。これは、トラフィックが非 ACI ネットワークを通過する必要がある場合（たとえば、Cisco APIC の管理下でないデバイスが通過するパケットの CoS 値を変更する可能性がある SD-WAN で区切られた複数のファブリック間）に必要です。

始める前に

- [vManage コントローラの追加 \(309 ページ\)](#) の説明に従って、vManage コントローラを NDO に追加する必要があります。
- ACI ファブリック内の Quality of Service (QoS) 機能に精通している必要があります。QoS の詳細については、[Cisco APIC and QoS](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

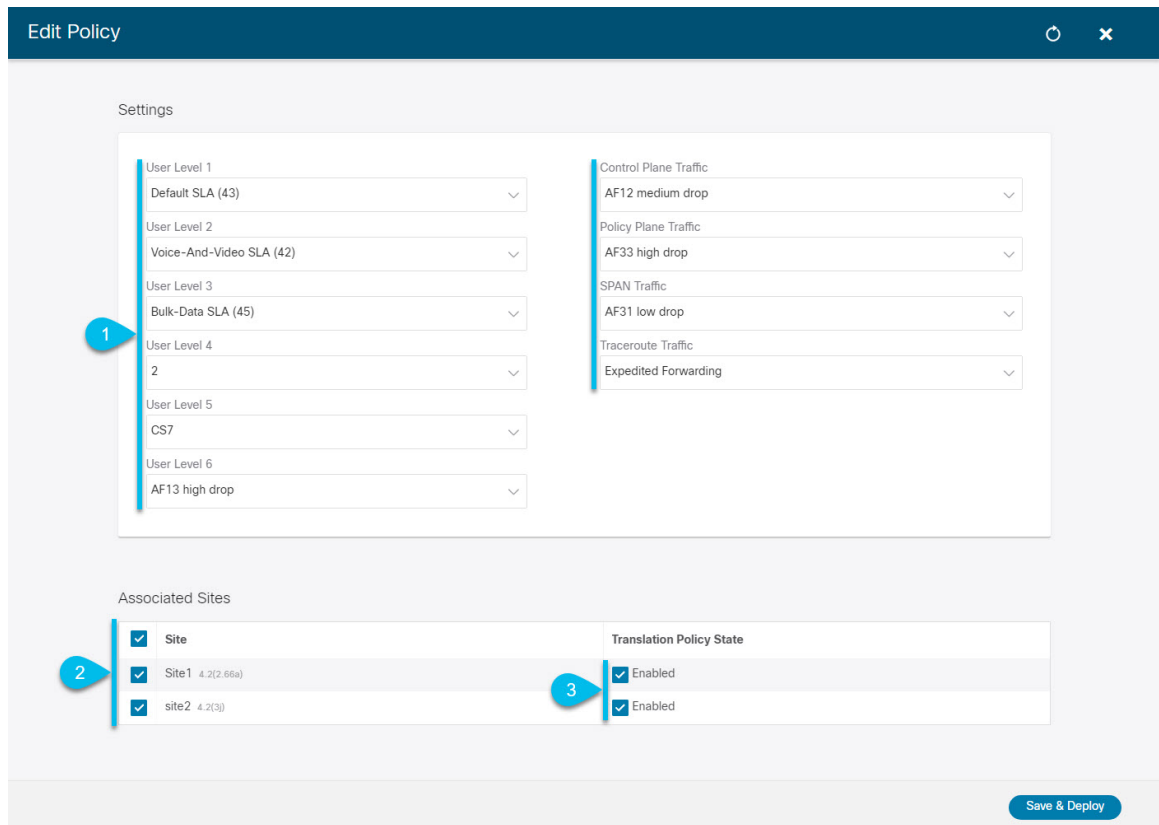
ステップ 2 グローバル DSCP ポリシー設定画面を開きます。



- a) [アプリケーション管理 (Application Management)] > [ポリシー (Policies)] の順に移動します。
- b) [グローバル DSCP ポリシー名 (Global DSCP Policy name)] をクリックします。

[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

ステップ 3 グローバル DSCP ポリシーを更新します。



- a) 各 ACI QoS レベルの DSCP 値を選択します。

各ドロップダウンには、使用可能な DSCP 値のデフォルトリストと、vManage SLA ポリシーからインポートされた値（Voice-And-Video SLA (42) など）が含まれます。

- b) ポリシーを展開するサイトを選択します。

エンドツーエンドの一貫した QoS 動作を実現するために、Multi-Site ドメインの一部であるすべてのサイトにポリシーを展開することを推奨します。

- c) 各サイトの展開時にポリシーを有効にするかどうかを選択します。
d) [保存して展開 (Save & Deploy)] をクリックします。

保存して展開すると、DSCP ポリシー設定が各サイトにプッシュされます。設定を確認するには、サイトの APIC にログインし、[テナント (Tenants)] > [インフラ (infra)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L3 トラフィックの DSCP クラス CoS 変換ポリシー (DSCP class-CoS translation policy for L3 traffic)] に移動します。

次のタスク

グローバル DSCP ポリシーを定義した後、の説明に従って、ECI またはコントラクトに ACI QoS レベルを割り当てることができます。[EPG およびコントラクトの QoS レベルの設定 \(312 ページ\)](#)

EPG およびコントラクトの QoS レベルの設定

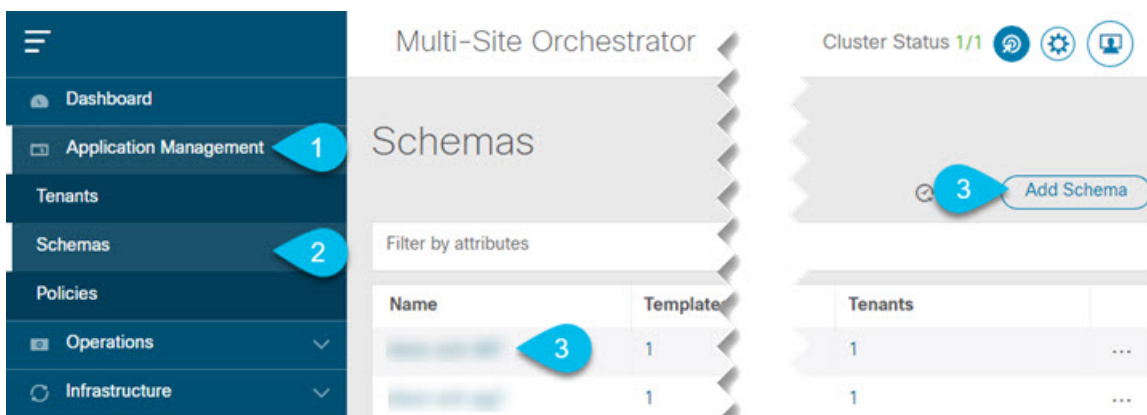
ここでは、ファブリック内のトラフィックの ACI QoS レベルを選択する方法について説明します。個々のコントラクトまたは EPG 全体に対して QoS を指定できます。

始める前に

- [vManage コントローラの追加 \(309 ページ\)](#) の説明に従って、vManage コントローラを NDO に追加する必要があります。
- [グローバル DSCP ポリシーの設定 \(310 ページ\)](#) の説明に従って、グローバル DSCP ポリシーを定義しておく必要があります。
- ACI ファブリック内の Quality of Service (QoS) 機能に精通している必要があります。QoS の詳細については、[Cisco APIC and QoS](#) を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

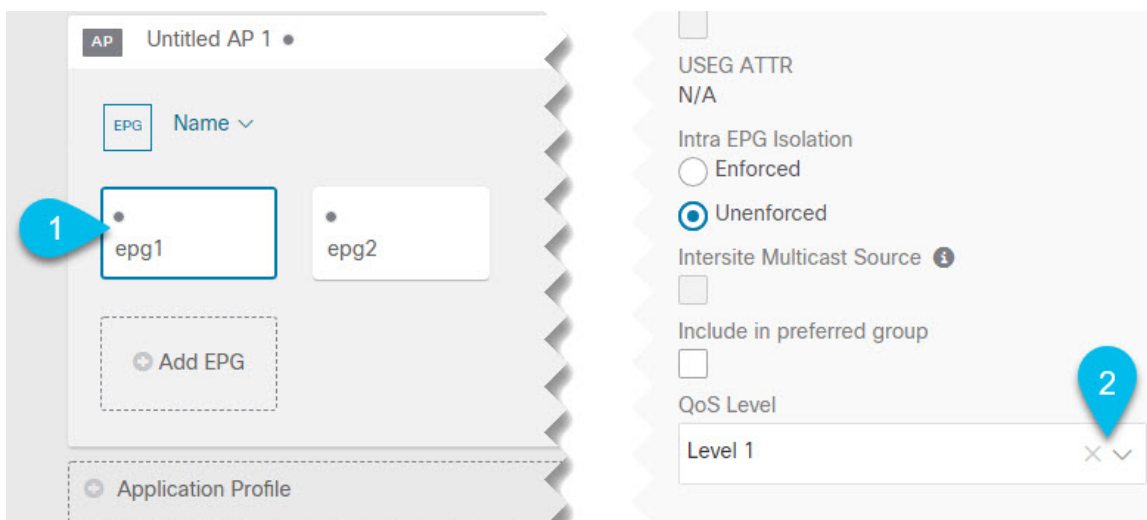
ステップ 2 編集するスキーマを選択します。



- [アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] > の順に移動します。
- 編集するスキーマの名前をクリックするか、[スキーマの追加 (Add Schema)] をクリックして新しいスキーマを作成します。

[スキーマの編集 (Edit Schema)] ウィンドウが開きます。

ステップ3 EPG の QoS レベルの選択



- メインペインで、[EPG] エリアまでスクロールダウンして EPG を選択するか、[EPG の追加 (Add EPG)] をクリックして新しい EPG を作成します。
- 右側のサイドバーで [QoS レベル (QoS Level)] ドロップダウンまでスクロールし、EPG に割り当てる QoS レベルを選択します。

EPGからのサイト間トラフィックがSD-WANネットワーク全体で目的のSLAで処理されるように、事前に設定されたグローバルDSCPポリシーに基づいてQoSレベルを選択する必要があります。

ステップ4 EPG の QoS レベルの選択

The screenshot displays the configuration interface for a contract. On the left, the 'CONTRACT' section is visible, showing a list with one item 'c1' and a '+ VRF' button. A blue callout box with the number '1' points to the 'c1' entry. Below this is the 'VRF' section with a list containing 'vrf1' and a '+ VRF' button. On the right, the 'Filter Chain' section shows a table with the following data:

Name	Directive
t1	none

Below the table is a '+ Filter' button. Underneath is the 'Service Graph' section with a dropdown menu showing 'Select or find an item here'. The 'ON-PREMISES PROPERTIES' section is highlighted with a grey background and contains a 'QoS Level' dropdown menu set to 'Level 1'. A blue callout box with the number '2' points to the 'Level 1' selection.

- メインペインで、[**コントラクト (Contract)**] 領域までスクロールダウンしてコントラクトを選択するか、[+] アイコンをクリックして新しいコントラクトを作成します。
- 右側のサイドバーで、[**QoS レベル (QoS Level)**] ドロップダウンまでスクロールし、コントラクトに割り当てる QoS レベルを選択します。

2つの EPG 間のサイト間トラフィックが SD-WAN ネットワーク全体で目的の SLA で処理されるように、事前に設定されたグローバル DSCP ポリシーに基づいて QoS レベルを選択する必要があります。



第 26 章

SR-MPLS 経由で接続されたサイト

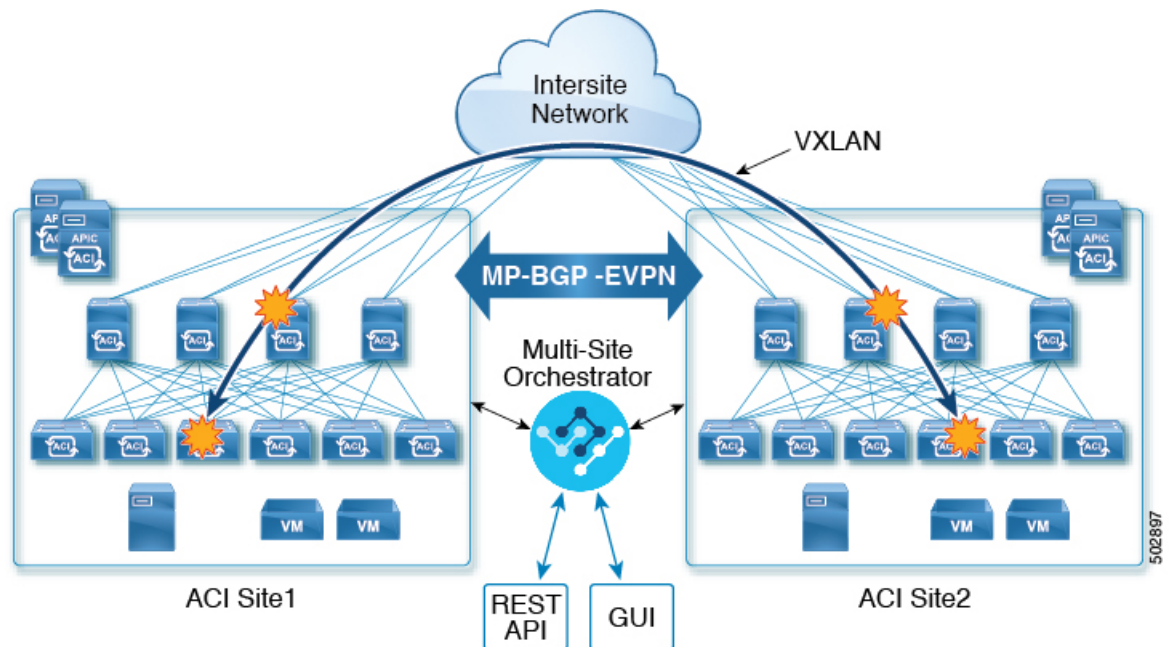
- [SR-MPLSおよびマルチサイト \(315 ページ\)](#)
- [インフラの設定 \(317 ページ\)](#)
- [SR-MPLS テナントの要件と注意事項 \(325 ページ\)](#)
- [SR-MPLS ルート マップ ポリシーの作成 \(328 ページ\)](#)
- [SR-MPLS 設定のテンプレートの有効化 \(330 ページ\)](#)
- [VRF および SR-MPLS L3Out の作成 \(330 ページ\)](#)
- [サイトローカル VRF 設定の構成 \(331 ページ\)](#)
- [サイトローカル SR-MPLS L3Out 設定の構成 \(332 ページ\)](#)
- [MPLS ネットワークにより区切られた EPG 間の通信 \(333 ページ\)](#)
- [設定の展開 \(334 ページ\)](#)

SR-MPLS およびマルチサイト

Nexus Dashboard Orchestrator、リリース 3.0(1) および APIC リリース 5.0(1) 以降では、マルチサイトアーキテクチャにより、MPLS ネットワークを介して、サイト数 APIC への接続がサポートされています。

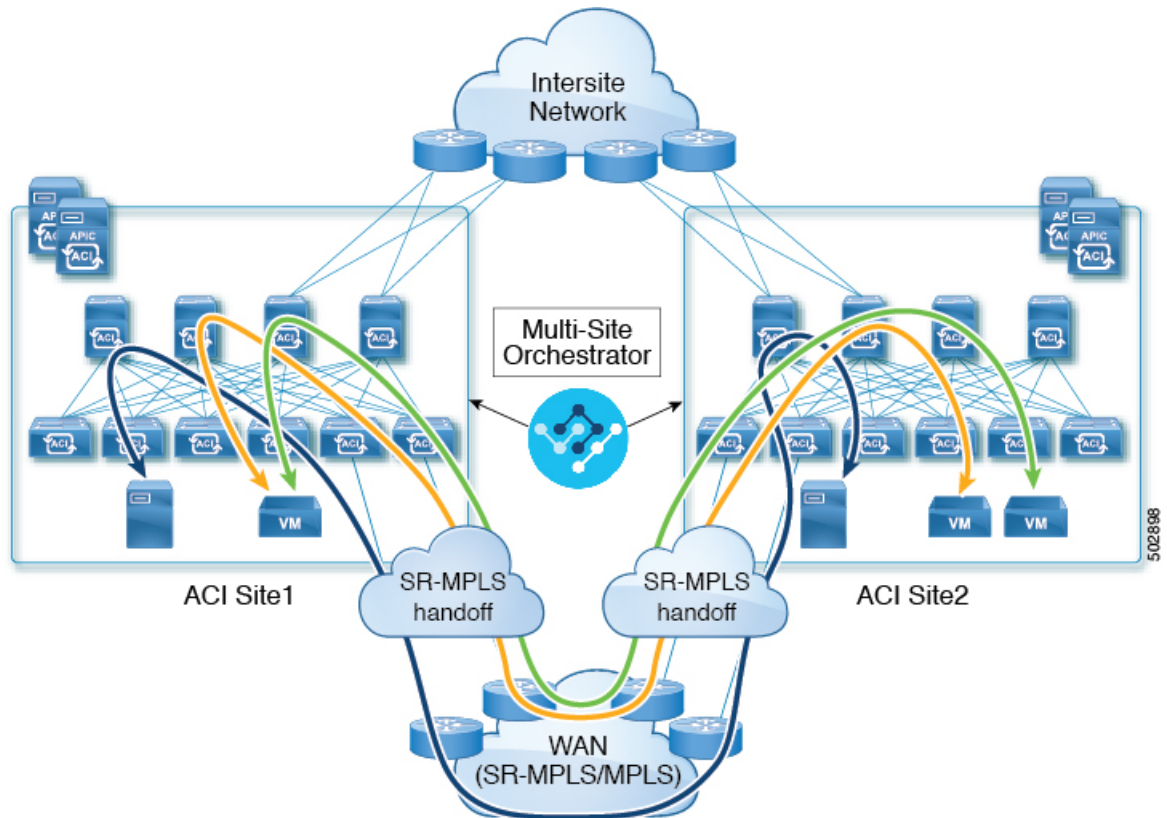
代表的な Multi-Site デプロイでは、サイト間トラフィックは、VXLAN カプセル化を介したサイト間ネットワーク (ISN) を通じて転送されます。

図 37: Multi-Site と ISN



リリース 3.0(1), MPLS ネットワークは、WAN を介したサイト間通信を許可する ISN に加えて、またはその代わりに使用できます。

図 38: Multi-Site と ISN



次のセクションでは、Nexus Dashboard Orchestrator からこれらのサイトにデプロイされるスキーマを管理するためのガイドライン、制限事項、およびそれ特定の設定について説明します。MPLS ハンドオフ、サポートされている個々のサイトのトポロジ(リモートリーフサポートなど)、ポリシーモデルは、『Cisco APIC Layer 3 ネットワーキング設定ガイド』で入手可能です。

インフラの設定

注意事項と制約事項

Nexus Dashboard Orchestrator により管理される SR-MPLS ネットワークに接続される APIC サイトを追加する場合、次のことにご留意ください。

- ノードの更新など、トポロジーへの変更は、[サイト接続性情報の更新 \(161 ページ\)](#) の説明に従ってサイトの構成が更新されるまで、Orchestrator 構成には反映されません。
- SR-MPLS ネットワークに接続されているサイトに展開されているオブジェクトとポリシーは、その他のサイトにストレッチできません。

テンプレートを作成し、テナントを指定するときに、テナントで SR-MPLS オプションを有効にする必要があります。これにより、そのテンプレートを単一の ACI サイトにのみマッピングできるようになります。

- SR-MMPLS ネットワークを通じて接続されているサイトに展開されているテナントは、SR-MPLS 設定に特別の固有の構成オプションのセットをもちます。テナント構成は、[Multi-Site 構成ガイド](#)、リリース 3.1(x) の「テナント管理」の章で説明されています。

サポート対象ハードウェア

SR-MPLS 接続は、以下のプラットフォームに対してサポートされています。

- ボーダー リーフ スイッチ：「FX」、「FX2」、および「GX」 スイッチ モデル。
- スパイン スイッチ：
 - ラインカード名の末尾に「LC-EX」、「LC-FX」、および「GX」が付いたモジュラスパイン スイッチ モデル。
 - Cisco Nexus 9000 シリーズ N9K-C9364C および N9K-C9332C 固定スパイン スイッチ。
- DC-PE ルータ：
 - Network Convergence System (NCS) 5500 シリーズ
 - ASR 9000 シリーズ
 - NCS 540 または 560 ルータ

SR-MPLS インフラ L3Out

次のセクションの説明に従って、SR-MPLS ネットワークに接続されたファブリックの SR-MPLS Infra L3Out を作成する必要があります。SR-MPLS L3Out Infra を作成するときには、次の制約が適用されます。

- 各 SR-MPLS L3Out Infra L3Out には固有の名前が必要です。
- 異なるルーティング ドメインに接続されているロケーションごとに複数の SR-MPLS Infra L3Out を持つこと、その際に同じボーダー リーフ スイッチは複数の L3Out にあること、各ルーティング ドメインに向かって VRF のルーティング ポリシーをエクスポートすることが可能です。
- ボーダー リーフ スイッチが複数の SR-MPLS Infra L3Out にあることができる場合でも、ボーダー リーフ スイッチ/プロバイダ エッジ ルーターの組み合わせは 1 つの SR-MPLS L3Out になければなりません。ユーザ VRF/ボーダー リーフ スイッチ/プロバイダ エッジ ルートの組み合わせに対して 1 つのルーティング ポリシーのみが存在できるからです。
- 複数のポッドおよびリモート ロケーションから SR-MPLS 接続を確立する必要がある場合は、SR-MPLS 接続を使用するポッドおよびリモート リーフ ロケーションのそれぞれに異なる SR-MPLS インフラ L3Out があることを確認します。

- ポッドの1つがSR-MPLS ネットワークに直接接続されていないマルチポッドまたはリモートリーフトポロジがある場合、SR-MPLS ネットワークを宛先とするそのポッドのトラフィックは、SR-MPLS L3Out を持つ別のポッドへの標準IPNパスを使用します。その後、トラフィックは他のポッドのSR-MPLS L3Out を使用して、SR-MPLS ネットワーク全体の宛先に到達します。
- 複数のVRFからのルートは、1つのSR-MPLS Infra L3Out から、このSR-MPLS Infra L3Out のノードに接続されているプロバイダエッジ (PE) ルーターにアドバタイズできます。PE ルータは、ボーダーリーフに直接接続することも、他のプロバイダー (P) ルータを介して接続することもできます。
- アンダーレイ設定は、1つのロケーションに対して複数のSR-MPLS Infra L3Out にわたって異なるか、同じ場合があります。たとえば、両方に対して別のプロバイダルーターに接続されたアンダーレイをもつ、ドメイン1のPE-1とドメイン2のPE-2に同じボーダーリーフスイッチが接続されていると想定します。この場合、2つのSR-MPLS Infra L3Out が作成されます。PE-1に対して1つとPE-2に対して1つです。しかしアンダーレイの場合、プロバイダルーターへの同じBGPピアになります。インポート/エクスポートルートマップは、ユーザVRFの対応するルートプロファイル設定に基づいて、PE-1およびPE-2へのEVPNセッションに設定されます。

MPLS スイッチングに関するガイドラインと制限事項

次に、MPLS QoS のデフォルトの動作を示します。

- 境界リーフスイッチ上のすべての受信MPLSトラフィックはQoSレベル3 (デフォルトのQoSレベル) に分類されます。
- 境界リーフスイッチは、再マーキングなしでSR-MPLSからのトラフィックの元のDSCP値を保持します。
- 境界リーフスイッチは、デフォルトのMPLSEXP (0) のパケットをSR-MPLSネットワークに転送します。

次に、MPLS カスタム QoS ポリシーを設定する際のガイドラインと制約事項を示します。

- データプレーンポリサー (DPP) は、SR-MPLS L3Out ではサポートされていません。
- レイヤ2 DPP は、MPLS インターフェイスの入力方向で動作します。
- レイヤ2 DPP は、出力カスタムMPLS QoS ポリシーがない場合、MPLS インターフェイスの出力方向で動作します。
- VRF レベルのポリシングはサポートされていません。

SR-MPLS QoS ポリシーの作成

このセクションでは、MPLS ネットワーク経由で接続されているサイトの SR MPLS QoS ポリシーを設定する方法について説明します。該当するサイトがない場合は、このセクションをスキップできます。

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの QoS レベル (Level13) がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値 (0) がファブリックから離れるパケットにマーキングされます。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [メインメニュー (Main menu)] で、[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] を選択します。

ステップ 3 メイン ペインで、[ポリシーの追加 (Add Policy)] > [QoS ポリシーの作成 (Create QoS Policy)] を選択します。

ステップ 4 [QoS ポリシーの追加 (Add QoS Policy)] 画面で、ポリシーの名前を入力します。

ステップ 5 入力 QoS 変換ルールを追加するには、[入カールの追加 (Add Ingress Rule)] をクリックします。

これらのルールは、MPLS ネットワークから ACI ファブリックに入力されるトラフィックに適用され、着信パケットの EXP ビット値を ACI QoS レベルにマッピングするため、また、パケットが ACI ファブリック内にある間に、VXLAN ヘッダーに DiffServ コードポイント (DSCP) 値を設定するためにも使用されます。

値は、境界リーフでカスタム QoS 変換ポリシーを使用して取得されます。再マーキングなしの SR-MPLS からのトラフィックの元の DSCP 値。カスタムポリシーが定義されていないか、一致していない場合、デフォルトの QoS レベル (Level13) が割り当てられます。

- a) [EXP 照合開始 (Match Exp From)] と [EXP 照合終了 (Match EXP To)] フィールドで、照合する入力 MPLS パケットの EXP 範囲を指定します。
- b) [キューの優先順位 (Queuing Priority)] ドロップダウンから、マッピングする ACI QoS レベルを選択します。

これは、ACI ファブリック内のトラフィックに割り当てる QoS レベルで、ACI はファブリック内のトラフィックのプライオリティを決めるために使用します。オプションの範囲は Level1 ~ Level6 です。デフォルト値は Level13 です。このフィールドで選択しない場合、トラフィックには自動的に Level13 の優先順位が割り当てられます。

- c) [DSCP 設定 (Set DSCP)] ドロップダウンから、パケットが ACI ファブリック内にある場合にパケットに割り当てる DSCP 値を選択します。

指定された DSCP 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を [未指定 (Unspecified)] に設定すると、パケットの元の DSCP 値が保持されます。

- d) **[Cos 設定(Set CoS)]** ドロップダウンから、パケットが ACI ファブリック内にある場合にパケットに割り当てる CoS 値を選択します。

指定された CoS 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を [未指定 (Unspecified)] に設定すると、パケットの元の CoS 値が保持されますが、これはファブリックで CoS 保存オプションが有効になっている場合のみです。CoS 保存の詳細については、「[Cisco APIC and QoS](#)」を参照してください。

- e) チェックマーク アイコンをクリックして、ルールを保存します。
f) 追加の入力 QoS ポリシー ルールについて、この手順を繰り返します。

ステップ 6 出力 QoS 変換ルールを追加するには、**[出力ルールの追加 (Add Egress Add Rule)]** をクリックします。

これらのルールは、MPLS L3Out 経由で ACI ファブリックから発信されるトラフィックに適用され、パケットの IPv4 DSCP 値を MPLS パケットの EXP 値および内部イーサネットフレームの CoS 値にマッピングするために使用されます。

分類は、EPG および L3Out トラフィックに使用される既存のポリシーに基づいて非境界リーフスイッチで行われます。カスタムポリシーが定義されていないか、一致していない場合、デフォルトの EXP 値 0 がすべてのラベルでマークされます。EXP 値は、デフォルト ポリシー シナリオとカスタム ポリシー シナリオの両方でマークされ、パケット内のすべての MPLS ラベルで行われます。

カスタム MPLS 出力ポリシーは、既存の EPG、L3out、および契約 QoS ポリシーをオーバーライドできません。

- a) **[DSCP 照合開始 (MATCH DSCP From)]** と **[DSCP 照合終了 (MATCH DSCP To)]**] ドロップダウンを使用して、出力 MPLS パケットのプライオリティを割り当てるために一致させる ACI ファブリックパケットの DSCP 範囲を指定します。
b) **[MPLS EXP の設定 (SET MPLS EXP)]** ドロップダウンから、出力 MPLS パケットに割り当てる EXP 値を選択します。
c) **[CoS の設定(Set CoS)]** ドロップダウンから、出力 MPLS パケットに割り当てる CoS 値を選択します。
d) チェックマーク アイコンをクリックして、ルールを保存します。
e) 追加の出力 QoS ポリシー ルールについて、この手順を繰り返します。

ステップ 7 **[保存 (Save)]** をクリックして、QoS ポリシーを保存します。

次のタスク

QoS ポリシーを作成したら、[#unique_204](#) の説明に従って mpls 接続を有効にし、MPLS L3Out を設定します。

SR-MPLS インフラ L3Out の作成

このセクションでは、SR-MPLS ネットワーク経由で接続されているサイトの SR-MPLS L3Out を設定する方法について説明します。

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP EVPN セッションを設定するために使用されます。
- SR-MPLS インフラ L3Out は、ポッドまたはリモートリーフスイッチサイトにスコープされます。
- 1 つの SR-MPLS インフラ L3Out 内の境界リーフスイッチまたはリモートリーフスイッチは、1 つ以上のルーティングドメイン内の 1 つ以上のプロバイダーエッジ (PE) ルータに接続できます。
- ポッドまたはリモートリーフスイッチサイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。

始める前に

次のものがが必要です。

- [Cisco ACI サイトの追加 \(147 ページ\)](#) で説明しているように、MPLS ネットワークを経由して接続されているサイトを追加したこと。
- 必要に応じ、[SR-MPLS QoS ポリシーの作成 \(320 ページ\)](#) で説明しているように、SR-MPLS QoS ポリシーを作成したこと。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 サイトで SR-MPLS 接続が有効になっていることを確認します。

- a) メインのナビゲーションメニューで、**[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infra Configuration)]** を選択します。
- b) **[インフラの設定 (Infra Configuration)]** ビューで、**[インフラ設定 (Configure Infra)]** をクリックします。
- c) 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。
- d) 右側の **[<サイト名> 設定 (Settings)]** ペインで、**[SR-MPLS 接続性 (SR-MPLS Connectivity)]** ノブを有効にして、セグメントルーティンググローバルブロック (SRGB) の範囲を指定します。

SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SID インデックス値は BGP-LU を使用してピアルータにアドバタイズされ、ピアルータは SID インデックスを使用してローカルラベルを計算します。

セグメントルーティンググローバルブロック (SRGB) は、ラベルスイッチングデータベース (LSD) でセグメントルーティング (SR) 用に予約されているラベル値の範囲です。SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SID インデックス値は BGP-LU を使用してピアルータにアドバタイズされ、ピアルータは SID インデックスを使用してローカルラベルを計算します。

デフォルトの範囲は 16000 ~ 23999 です。

ステップ 3 メインのペインで、ポッド内の **[+SR-MPLS L3Out の追加 (+Add SR-MPLS L3Out)]** をクリックします。

ステップ 4 右側の **[プロパティ (Properties)]** ペインで、SR-MPLS L3Out の名前を入力します。

ステップ5 (任意) **[QoS ポリシー (QoS Policy)]** ドロップダウンで、MPLS トラフィックのために作成した QoS ポリシーを選択します。

SR-MPLS QoS ポリシーの作成 (320 ページ) で作成した QoS ポリシーを選択します。

それ以外の場合、カスタムQoSポリシーを割り当てないと、次のデフォルト値が割り当てられます。

- 境界リーフ スイッチ上のすべての着信 MPLS トラフィックは、QoS レベル 3 (デフォルトの QoS レベル) に分類されます。
- 境界リーフ スイッチは次の処理を実行します。
 - 再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
 - CoS 保存が有効な場合、テナントトラフィックの元の CoS 値を使用してパケットを MPLS ネットワークに転送します。
 - デフォルトの MPLS EXP 値 (0) のパケットを SR-MPLS ネットワークに転送します。
- また、境界リーフ スイッチは、SR ネットワークへの転送中に、アプリケーション サーバから着信するテナントトラフィックの元の DSCP 値を変更しません。

ステップ6 **[L3 ドメイン (L3 Domain)]** ドロップダウンで、レイヤ 3 ドメインを選択します。

ステップ7 BGP 設定を構成します。

サイトの境界リーフ (BL) スイッチとプロバイダエッジ (PE) ルータ間の BGP EVPN 接続について、BGP 接続の詳細を指定する必要があります。

- a) **[+BGP 接続の追加 (+Add BGP Connectivity)]** をクリックします。
- b) **[BGP 接続の追加 (Add BGP Connectivity)]** ウィンドウで詳細を入力します。

[MPLS BGP-EVPN ピア IPv4 アドレス (MPLS BGP-EVPN Peer IPv4 Address)] フィールドで、DC-PE ルータのループバック IP アドレスを入力します。このルータは必ずしも、境界リーフに直接接続されているデバイスとは限りません。

[リモート AS 番号 (Remote AS Number)] に、DC-PE のネイバー自律システムを一意に識別する番号を入力します。自律システム番号は 4 バイトで、1 ~ 4294967295 のプレーン形式で指定します。ACI は asplain 形式のみをサポートし、asdot または asdot+ 形式の AS 番号はサポートしないことに注意してください。ASN 形式の詳細については、『[Explaining 4-Byte Autonomous System \(AS\) ASPLAIN and ASDOT Notation for Cisco IOS](#)』を参照してください。

[TTL] フィールドで、境界リーフと DC-PE ルータ間の複数のホップ数を考慮に入れて、十分大きな値を指定します。たとえば 10 とします。許容範囲は 2 ~ 255 ホップです。

(任意) 展開に基づいて追加の BGP オプションを有効にします。

- c) **[保存 (Save)]** をクリックして BGP 設定を保存します。
- d) 追加の BGP 接続があれば、このステップを繰り返します。

通常、2 つの DC-PE ルータに接続することになるので、両方の接続について BGP ピア情報を入力します。

ステップ8 境界リーフ スイッチと、SR-MPLS ネットワークに接続されているポートの設定を構成します。

境界リーフ スイッチについての情報、そして SR-MPLS ネットワークに接続されているインターフェイス ポートの情報を入力する必要があります。

- a) **[+リーフの追加 (+Add Leaf)]** をクリックして、リーフ スイッチを追加します。
- b) **[リーフの追加 (Add Leaf)]** ウィンドウで、**[リーフ名 (Leaf Name)]** ドロップダウンからリーフ スイッチを選択します。
- c) 有効なセグメント ID (SID) オフセットを入力します。

このセクションの後の部分で、インターフェイスポートを設定する際には、セグメントルーティングを有効にするかを選択できます。SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SID インデックス値は BGP-LU を使用してピア ルータにアダプタイズされ、ピア ルータは SID インデックスを使用してローカル ラベルを計算します。セグメントルーティングを使用する予定の場合には、この境界リーフのセグメント ID を指定する必要があります。

- 値は、先ほど設定した SRGB の範囲内である必要があります。
- この値は、サイト内のすべての SR-MPLS L3Out で選択したリーフスイッチで同じ必要があります。
- すべてのサイトの複数のリーフに同じ値を使用することはできません。
- 値を更新する必要がある場合は、まず、リーフ内のすべての SR-MPLS L3Out から値を削除し、設定を再展開する必要があります。その後、新しい値で更新し、新しい設定を再展開できます。

- d) ローカルの **[ルータ ID (Router ID)]** を入力します。

ファブリック内で一意なルータ 識別子です。

- e) **[BGP EVPN ループバック (BGP EVPN Loopback)]** アドレスを入力します。

BGP-EVPN ループバックが BGP-EVPN コントロールプレーンセッションに使用されます。このフィールドを使用して、境界リーフ スイッチの EVPN ループバックと DC-PE 間の MP-BGP EVPN セッションを設定し、オーバーレイプレフィックスをアダプタイズします。MP-BGP EVPN セッションは、BP-EVPN ループバックと BGP-EVPN リモートピアアドレスの間で確立されます。このアドレスは、**[BGP-EVPN リモート IPv4 アドレス (BGP-EVPN Remote IPv4 Address)]** フィールドで設定します (前の BGP 接続のステップ)。

BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

- f) **[MPLS トランスポート ループバック (MPLS Transport Loopback)]** アドレスを入力します。

MPLS トランスポート ループバックは、ACI 境界リーフ スイッチと DC-PE 間のデータ プレーンセッションを構築するために使用されます。MPLS トランスポート ループバックは、境界リーフ スイッチから DC-PE ルータにアダプタイズされるプレフィックスのネクスト ホップになります。

BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

- g) **[インターフェイスの追加 (Add Interface)]** をクリックして、スイッチ インターフェイスの詳細を入力します。

[インターフェイスのタイプ (Interface Type)] ドロップダウンから、通常のインターフェイスなのか、それともポートチャネルなのかを選択します。ポートチャネルインターフェイスを使用する場合には、それ以前に APIC 上で作成しておく必要があります。

それからインターフェイス、その IP アドレス、および MTU サイズを入力します。サブインターフェイスを使用する場合には、サブインターフェイスの **[VLAN ID]** を入力します。それ以外の場合には **[VLAN ID]** フィールドはブランクのままにします。

[BGP ラベルユニキャストピア IPv4 アドレス (BGP-Label Unicast Peer IPv4 Address)] および **[BGP ラベルユニキャストリモート AS 番号 (BGP-Label Unicast Remote AS Number)]** で、ネクストホップデバイス (インターフェイスに直接接続されているデバイス) の BGP-LU ピア情報を指定します。ネクストホップアドレスは、インターフェイスで設定したサブネットの一部である必要があります。

セグメントルーティング (SR) MPLS を有効にするかどうかを選択します。

(任意) 展開に基づいて追加の BGP オプションを有効にします。

最後に、**[インターフェイスタイプ (Interface Type)]** ドロップダウンの横にあるチェックマークをクリックして、インターフェイスポート情報を保存します。

- h) MPLS ネットワークに接続されているスイッチのすべてのインターフェイスについて、前のサブステップを繰り返します。
- i) **[保存 (Save)]** をクリックして、リーフスイッチ情報を保存します。

ステップ 9 MPLS ネットワークに接続されているすべてのリーフスイッチについて、前のステップを繰り返します。

次のタスク

MPLS 接続を有効にして設定したら、[『マルチサイトコンフィギュレーションガイド、リリース 3.0\(x\)』](#) に説明されている方法で、テナント、ルートマップ、およびスキーマを作成し、管理することができます。

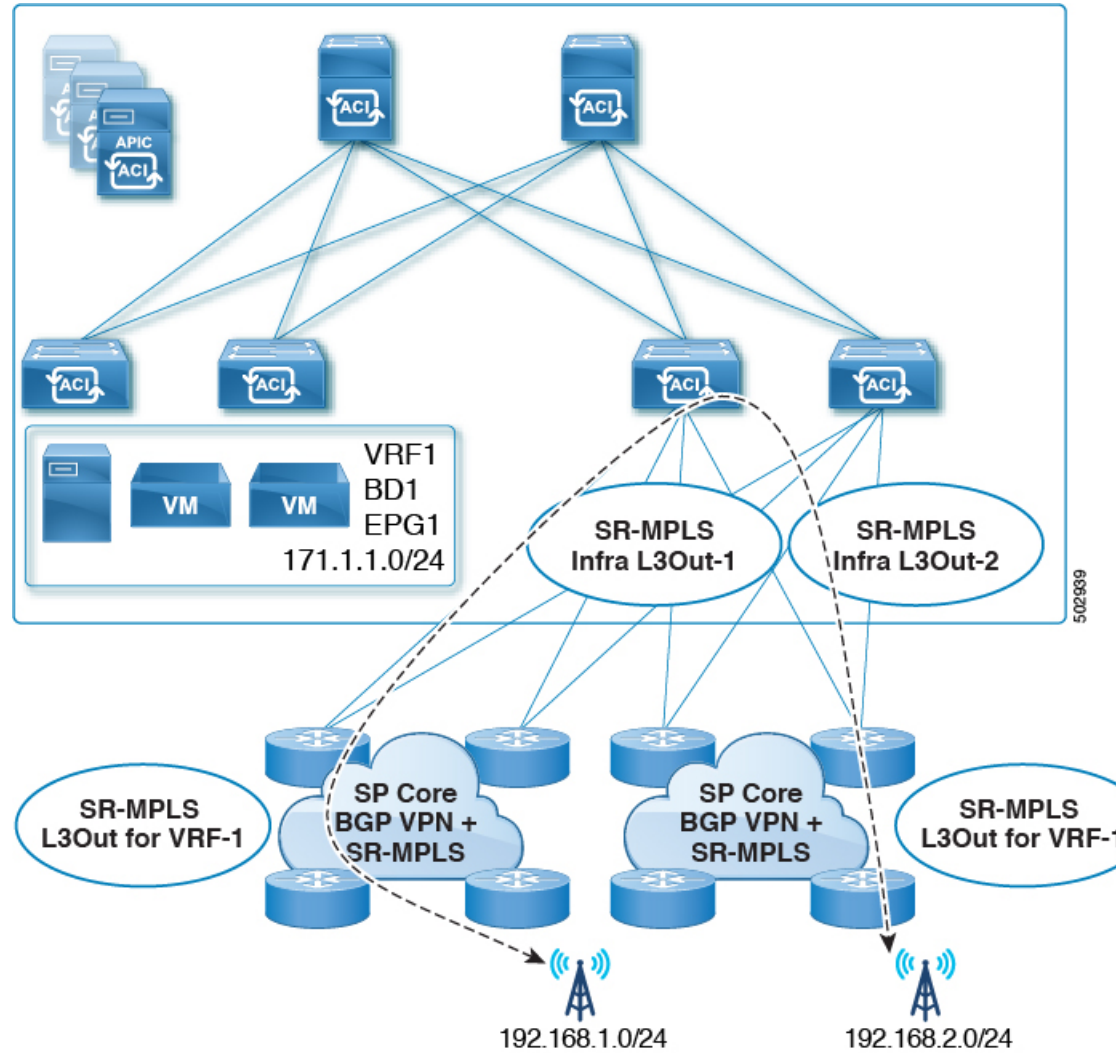
SR-MPLS テナントの要件と注意事項

Infra MPLS の設定と要件は Day-0 操作の章で説明されていますが、次の制約が SR-MPLS ネットワークに接続されているし後に展開するユーザテナントに適用されます。

- Day-0 操作の章で説明されているとおり、QoS ポリシーを含む SR-MPLS Infra L3Outs を作成し、設定します。
- ファブリックの 2 つの EPG 間のトラフィックが SR-MPLS ネットワークを通過する必要がある場合:
 - 各 EPG とローカル SR-MPLS L3Out で定義された外部 EPG の間に、コントラクトを割り当てる必要があります。

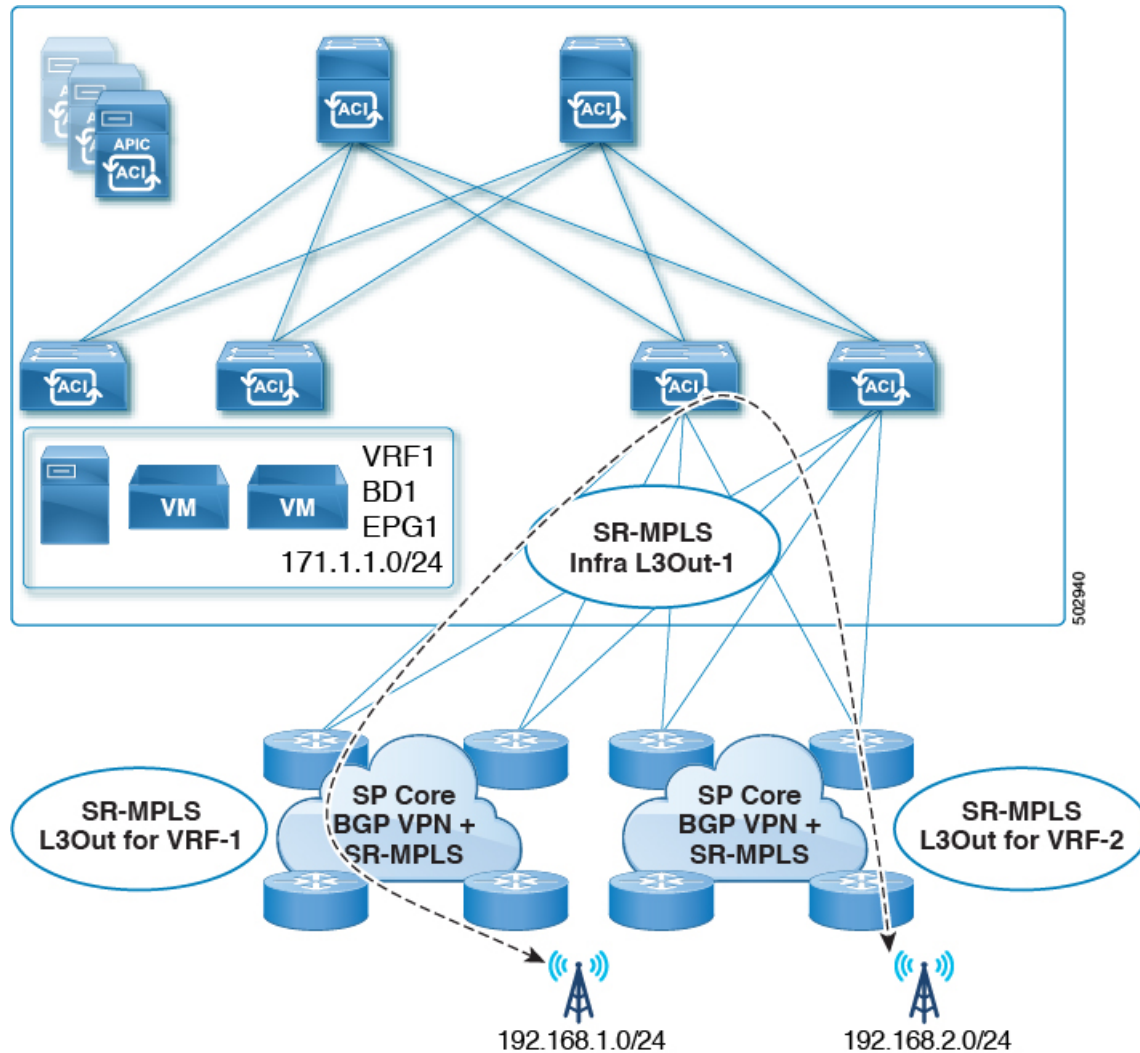
- 両方の EPG が同じ ACI ファブリックの一部であるが、SR-MPLS ネットワークによって分離されている場合（たとえば、マルチポッドまたはリモートリーフの場合）、EPG が異なる VRF に属していること、その間にはコントラクトがないこと、ルーティングが設定されていないことが必要です。
- EPG が異なるサイトにある場合、それらは同じ VRF に存在できますが、それらの間で直接設定されたコントラクトがあっては**なりません**。
EPG が異なるサイトにある場合、各 EPG は単一サイトにのみ展開する必要があることにご留意ください。サイト間の EPG の拡張は、SR-MPLS L3Outs を使用するときにはサポートされていません。
- SR-MPLS L3Out のルート マップ ポリシーを設定する場合:
 - 各 L3Out は、単一のエクスポート ルート マップがなければなりません。オプションで、単一のインポート ルート マップももつことができます。
 - SR-MPLS L3Out に関連付けられたルート マップは、SR-MPLS L3Out からアドバタイズする必要がある、ブリッジドメイン サブネットを含むすべてのルートを明示的に定義する必要があります。
 - 0.0.0.0/0 プレフィックスを定義し、ルートをアグリゲートしないことにした場合、デフォルトのルートのみを許可します。
しかし、ルート 0 ~ 32 を 0.0.0.0/0 プレフィックスにアグリゲートすることにした場合、VRF のすべてのトラフィックが許可されます。
 - 任意のルーティングポリシーを任意のテナント L3Out に関連付けることができます。
- 移行ルーティングがサポートされますが、一部の制約があります。
 - 同じ VRF を使用する 2 つの SR-MPLS ネットワーク間の移行ルーティングはサポートされていません。次の図は、サポートされていない設定の例を示します。

図 39: 単一の VRF を使用するサポートされていない移行ルーティング設定



- 異なる VRF を使用する 2 つの SR-MPLS ネットワーク間の移行ルーティングはサポートされています。次の図は、サポートされている設定の例を示します。

図 40:異なる VRF を使用するサポートされている移行ルーティング設定



SR-MPLS ルート マップ ポリシーの作成

このセクションでは、ルートマップポリシーを作成する方法について説明します。ルートマップは、テナントSR-MPLS L3Outからアドバタイズされるルートを指定できる `if-then` ルールのセットです。ルートマップでは、DC-PE ルータから受信したどのルートを BGP VPNv4 ACI コントロールプレーンに挿入するかを指定することもできます。

MPLS ネットワークに接続されているサイトがない場合は、このセクションをスキップできます。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

- ステップ2 [メインメニュー (Main menu)] で、[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] を選択します。
- ステップ3 メインペインで、[ポリシーの追加 (Add Policy)] > [ルートマップポリシーの作成 (Create Route Map Policy)] を選択します。
- ステップ4 [ルートマップポリシーの追加 (Add Route Map Policy)] 画面で、テナントを選択し、ポリシーの名前を指定します。
- ステップ5 ルートマップエントリを追加するには、[ルートマップエントリの順序 (Route-Map Entry Order)] の下の [エントリの追加 (add Entry)] をクリックします。

- a) [コンテキストの順序 (Context Order)] と [コンテキストアクション (Context Action)] を指定します。

各コンテキストは、1つ以上の一致基準に基づいてアクションを定義するルールです。

コンテキストの順序は、コンテキストが評価される順序を決定するために使用されます。値は 0 ~ 9 の範囲内である必要があります。

[アクション (Action)] は、一致が検出された場合に実行するアクション (許可 (permit) または拒否 (deny)) を定義します。

- b) IP アドレスまたはプレフィックスに基づいてアクションを照合する場合は、[IP アドレスの追加 (Add IP Address)] をクリックします。

[プレフィックス (prefix)] フィールドに、IP アドレスプレフィックスを入力します。IPv4 と IPv6 の両方のプレフィックスがサポートされています (例: 2003:1:1a5:1a5::/64 または 205.205.0.0/16)。

特定の範囲の IP を集約する場合は、[集約 (aggregate)] チェックボックスをオンにして、範囲を指定します。たとえば、0.0.0.0/0 プレフィックスを指定し、ルート 0 ~ 32 を集約するよう選択できます。

- c) コミュニティリストに基づいてアクションを照合する場合は、[コミュニティの追加 (Add community)] をクリックします。

[コミュニティ (Community)] フィールドに、コミュニティ文字列を入力します。たとえば、`regular:as2-as2-nn2:200:300` などです。

次に、[範囲 (Scope)] を選択します。

- d) [+ アクションの追加 (+Add Action)] をクリックして、コンテキストが一致する必要があるアクションを指定します。

次のアクションのうちの 1 つを選択できます。

- コミュニティの設定
- ルート タグの設定
- ウェイトの設定
- ネクスト ホップの設定
- プリファレンスの設定
- メトリックの設定
- メトリック タイプの設定

アクションを設定したら、チェックマーク アイコンをクリックしてアクションを保存します。

- e) (オプション) 前のサブステップを繰り返して、同じコンテキスト エントリ内で複数の一致基準とアクションを指定できます。
- f) **[保存 (save)]** をクリックして、コンテキスト エントリを保存します。

ステップ 6 (オプション) 同じルート ポリシーに複数のエントリを追加する場合は、前の手順を繰り返します。

ステップ 7 **[保存 (Save)]** をクリックして、ルート マップ ポリシーを保存します。

SR-MPLS 設定のテンプレートの有効化

MPLS を介して接続されたサイトに展開する際に固有のテンプレート構成設定がいくつかあります。テナントの SR MPLS を有効にすると、MPLS サイトで使用できない特定の設定を制限およびフィルタ処理し、そのようなサイトでのみ使用可能な追加の設定を行うことができます。

MPLS 固有の設定を更新する前に、テンプレートのテナントプロパティで **SR-MPLS** ノブを有効にする必要があります。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 メインのナビゲーションメニューで、**[Application Management (アプリケーション管理)] > [スキーマ (Schemas)]** を選択します。

ステップ 3 新規作成するか、または SR-MPLS テナントを設定する既存のスキーマを選択します。

ステップ 4 テナントを選択します。

新しいスキーマを作成した場合は、通常と同じようにテナントを選択します。それ以外の場合は、左側のサイドバーで既存のテンプレートをクリックします。

ステップ 5 右側のサイドバーの **テンプレート** のプロパティで、**SR MPLS** ノブを有効にします。

VRF および SR-MPLS L3Out の作成

このセクションでは、MPLS ネットワークで区切られるアプリケーション EPG 間の通信を設定するために使用する VRF、テナント SR-MPLS L3Out、および External EPG を作成する方法を説明します。

始める前に

次のことが必要です。

- [SR-MPLS 設定のテンプレートの有効化 \(330 ページ\)](#) で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。

ステップ 1 テンプレートを選択します。

ステップ 2 VRF を作成します。

- a) メインペインで、**VRF** エリアまで下方にスクロールして、+ 記号をクリックして VRF を追加します。
- b) 右のプロパティのサイドバーでは、VRF の名前を指定します。

ステップ 3 SR-MPLS L3Out を作成します。

- a) メイン ペインで、**SR-MPLS L3Out** エリアまで下方にスクロールして、+ 記号をクリックして L3Out を追加します。
- b) 右のプロパティのサイドバーでは、L3Out の名前を指定します。
- c) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップの外部 EPG に対して選択した同じ VRF を選択します。

ステップ 4 外部 EPG を作成します。

- a) メイン ペインで、**[外部 EPG (External EPG)]** エリアまで下方にスクロールし、+ 記号をクリックして外部 EPG を追加します。
- b) 右のプロパティのサイドバーでは、外部 EPG の名前を指定します。
- c) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップで作成された VRF を選択します。

サイトローカル VRF 設定の構成

SR-MPLS L3Out によって使用される VRF のための BGP ルート情報を設定する必要があります。

始める前に

次のことが必要です。

- [SR-MPLS 設定のテンプレートの有効化 \(330 ページ\)](#) で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。
- [VRF および SR-MPLS L3Out の作成 \(330 ページ\)](#) で説明しているように、VRF と SR-MPLS L3Out を作成していること。
- MPLS サイトにテンプレートを追加していること。

ステップ 1 テンプレートを含むスキーマを選択します。

ステップ 2 スキーマビューの左サイドバーの **[サイト (Sites)]** の下で、サイトローカルプロパティを編集するためにテンプレートを選択します。

ステップ 3 メインペインで、**[VRF]** エリアまで下にスクロールし、VRF を選択します。

ステップ 4 右プロパティサイドバーで、**[+BGP ルート ターゲット アドレスを追加 (+Add BGP Route Target Address)]** をクリックします。

ステップ 5 BGP 設定を構成します。

- a) **[アドレス ファミリ (Address Family)]** ドロップダウンから、その IPv4 または IPv6 アドレスを選択します。
- b) **[ルート ターゲット (Route Target)]** フィールドで、ルート文字列を設定します。
たとえば、`route-target:ipv4-nn2:1.1.1.1:1901` のようにします。
- c) **[タイプ (Type)]** ドロップダウンで、ルートをインポートするのか、それともエクスポートするのかを選択します。
- d) **[保存 (Save)]** をクリックして、ルート情報を保存します。

ステップ 6 (オプション) 上記のステップを繰り返して、その他の BGP ルート ターゲットを追加します。

サイトローカル SR-MPLS L3Out 設定の構成

通常の外部 EPG のサイトローカル L3Out プロパティを設定する場合と同じように、MPLS で接続されているサイトに展開される外部 EPG の SR-MPLS L3Out の詳細を設定する必要があります。

始める前に

次のことが必要です。

- [SR-MPLS 設定のテンプレートの有効化 \(330 ページ\)](#) で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。
- [VRF および SR-MPLS L3Out の作成 \(330 ページ\)](#) で説明しているように、VRF と SR-MPLS L3Out を作成していること。
- [サイトローカル VRF 設定の構成 \(331 ページ\)](#) で説明しているように、VRF のサイトローカルプロパティを設定していること。
- MPLS サイトにテンプレートを追加していること。

ステップ 1 テンプレートを含むスキーマを選択します。

ステップ 2 スキーマビューの左サイドバーの **[サイト (Sites)]** の下で、サイトローカルプロパティを編集するためにテンプレートを選択します。

ステップ 3 メインペインで、**[SR-Mpls L3Out]** エリアまで下にスクロールし、MPLS L3Out を選択します。

ステップ 4 右のプロパティサイドバーで、**[+SR-MPLS ロケーションの追加 (+Add SR-MPLS Location)]** をクリックします。

ステップ 5 SR-MPLS のロケーションの設定を構成します。

- a) **[SR-MPLS のロケーション (SR-MPLS Location)]** ドロップダウンで、そのサイトのインフラを設定する際に作成したインフラ SR-MPLS L3Out を選択します。
- b) **[外部 EPG (External EPGs)]** セクションで、ドロップダウンから外部 EPG を選択し、チェックマークのアイコンをクリックして追加します。
外部 EPG は複数追加できます。
- c) **[ルートマップポリシー (Route Map Policy)]** セクションの下で、前のセクションで作成したルートマップポリシーをドロップダウンから選択し、ルートをインポートするかエクスポートをするかを指定してから、チェックマークのアイコンをクリックして追加します。
1つのエクスポートルートマップポリシーを設定する必要があります。オプションとして、追加のインポートルートマップポリシーを設定することができます。
- d) **[保存 (Save)]** をクリックして、ロケーションを MPLS L3Out に追加します。

ステップ 6 (オプション) 前のステップを繰り返して、その他の SR-MPLS ロケーションを SR-MPLS L3Out に追加します。

MPLS ネットワークにより区切られた EPG 間の通信

通常、2つの EPG 間の通信を確立するには、1つの EPG をプロバイダに、もう1つをコンシューマとし、両方の EPG に同じコントラクトを割り当てるだけです。

しかし、2つの EPG が MPLS ネットワークで区切られている場合には、トラフィックはそれぞれの EPG の MPLS L3Out を通らなければならないので、コントラクトは、それぞれの EPG と、その MPLS L3Out の間に確立します。この動作は、EPG が異なるファブリックに展開されている場合でも、マルチポッドまたはリモードリーフの場合のように、同じサイトに展開されている場合でも、SR-MPLS ネットワークで区切られている場合でも同じです。

始める前に

次のことが必要です。

- MPLS ネットワークに接続されている 1つ以上のサイトを Orchestrator に追加していること。
- インフラ MPLS の設定を、「ゼロデイ オペレーション」の章で説明しているように構成していること。
- [SR-MPLS 設定のテンプレートの有効化 \(330 ページ\)](#) で説明されているとおり、スキーマを作成し、テナントを追加し、SR-MPLS に対してテナントを有効にしていること。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 通常のように、2つのアプリケーション EPG を作成します。

たとえば、epg1 および epg2 とします。

ステップ 3 2つの独立した外部 EPG を作成します。

これらの EPG は、特定の導入シナリオに応じて、同じテンプレートに含めることも、異なるテンプレートに含めることもできます。

たとえば、mpls-extepg-1 および mpls-extepg-2 とします。

ステップ 4 2つの個別のテナント SR-MPLS L3Out を設定します。

たとえば、mpls-13out-1 および mpls-13out-2 とします。

各テナント SR-MPLS L3Out について、[サイトローカル VRF 設定の構成 \(331 ページ\)](#) および [サイトローカル SR-MPLS L3Out 設定の構成 \(332 ページ\)](#) の説明に従って、VRF、ルートマップポリシー、および外部 EPG を設定します。

ステップ 5 ステップ 2 で作成した、2つのアプリケーション EPG の間のトラフィックを許可するために使用するコントラクトを作成します。

通常のように、コントラクトのためのフィルタを作成して定義する必要があります。

ステップ 6 コントラクトを適切な EPG に割り当てます。

作成した 2つのアプリケーション EPG 間のトラフィックを許可するため、実際にはコントラクトを 2 回割り当てる必要があります。epg1 とその mpls-13out-1 の間、そして epg2 とその mpls-13out-2 の間です。

例として、epg1 が epg2 にサービスを提供する場合、次のようにします。

- a) epg1 にタイプ `consumer` でコントラクトを割り当てます。
- b) mpls-13out-1 にタイプ `consumer` でコントラクトを割り当てます。
- c) epg2 にタイプ `consumer` でコントラクトを割り当てます。
- d) mpls-13out-1 にタイプ `consumer` でコントラクトを割り当てます。

設定の展開

1つの例外を除いて、構成テンプレートを通常どおり MPLS サイトに展開できます。MPLS サイトと別のサイトの間でオブジェクトとポリシーを拡張することはできないため、テンプレートを展開するときに選択できるサイトは 1 つだけです。

ステップ 1 テンプレートを展開するサイトを追加します。

- a) [スキーマ (Schema)] 表示の左側のサイドバーで、[サイト (Sites)] の下の + アイコンをクリックします。
- b) [サイトの追加 (Add Sites)] ウィンドウで、テンプレートを展開するサイトを選択します。

テンプレートが MPLS 対応の場合、単一サイトのみを選択できます。

- c) [テンプレートへの割り当て (Assign to Template)] ドロップダウンからスキーマを作成した 1 つ以上のテンプレートを選択します。
- d) [保存 (Save)] をクリックして、サイトを追加します。

ステップ2 設定を展開する

- a) [スキーマ (Schemas)] 表示のメイン ペインで、[サイトに展開 (Deploy to Sites)] をクリックします。
 - b) [サイトに展開 (Deploy to Sites)] ウィンドウで、サイトにプッシュされる変更を検証し、[展開 (Deploy)] をクリックします。
-



第 27 章

vzAny コントラクト

- [vzAny および Multi-Site \(337 ページ\)](#)
- [vzAny およびマルチサイトのガイドラインと制限事項 \(338 ページ\)](#)
- [コントラクトとフィルタの作成 \(340 ページ\)](#)
- [コントラクトを消費または提供するための vzAny の設定 \(341 ページ\)](#)
- [vzAny VRF の一部として EPG を作成する \(342 ページ\)](#)
- [自由な VRF 間通信 \(343 ページ\)](#)
- [多対 1 の通信 \(349 ページ\)](#)

vzAny および Multi-Site

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

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



(注) L3Out に関連付けられ、VRF の一部である外部 EPG も vzAny 論理グループに含まれます。

利点

Cisco ACI のポリシー情報は、ファブリックスイッチの TCAM テーブルにプログラムされています。TCAM エントリは、一般的に、コントラクト経由で互いに通信することを許可する EPG

の各ペアに固有の特定のものです。このことは、同じコントラクトが再使用された場合でも、複数の TCAM エントリが EPG の各ペアに対して作成されることを意味します。

ポリシー TCAM テーブルのサイズは、使用しているスイッチの生成に応じて異なります。特定の大規模環境では、ポリシーTCAMの使用を考慮し、制限を超えないようにすることが重要です。

vzAny を使用すると、同じ VRF 内のすべての EPG を単一の「グループ」に結合し、単一の TCAM エントリのみを消費しながら、グループ内の個々の EPG ではなく、そのグループとのコントラクト関係を作成できます。これにより、TRF スペースだけでなく、VRF 内の個々の EPG の複数のコントラクト関係の作成に費やす時間を節約できます。

使用例

vzAny には次の 2 つの代表的な使用例があります。

- [自由な VRF 間通信 \(343 ページ\)](#) に記載されているとおり、同じ VRF 内の EPG 間の自由な通信。
- [多対 1 の通信 \(349 ページ\)](#) で詳細に説明するように、多対 1 の通信により、同じ VRF 内のすべての EPG が単一の EPG から共有サービスを利用できるようになります。

vzAny およびマルチサイトのガイドラインと制限事項

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

- 特定の VRF の vzAny オブジェクトを有効にして契約を提供または消費することを計画している場合は、次の追加の制限が適用されます。
 - 特定の VRF の vzAny が契約 c1 のコンシューマとして設定されている場合、他の VRF の vzAny オブジェクトを c1 のプロバイダーとして設定してはなりません。
 - 特定の VRF の vzAny が契約 c1 のプロバイダーとして設定されている場合、他の VRF の vzAny オブジェクトを c1 のコンシューマとして設定してはなりません。
 - 特定の VRF の外部 EPG 部分がコントラクト c1 を使用している場合、他の VRF の vzAny オブジェクトを c1 のプロバイダーとして設定してはなりません。
 - 特定の VRF の EPG 部分がコントラクト c1 を使用している場合、他の VRF の vzAny オブジェクトを c1 のプロバイダーとして設定してはなりません。
 - 特定の VRF の vzAny がコントラクト c1 のプロバイダーとして設定されている場合、EPG、外部 EPG、または他の VRF の vzAny オブジェクトを c1 のコンシューマとして設定してはなりません。
- 特定の VRF の EPG および外部 EPG オブジェクトは、その VRF の vzAny がすでにコントラクトを使用または提供している場合、優先グループの一部として設定しないでください。

- 特定の VRF 内の EPG または外部 EPG オブジェクトがクラウドサイトに展開されている場合、その VRF の vzAny を設定してコントラクトを消費または提供することはできません。
- vzAny は、ファブリックが Cisco ACI 5.2(4) リリース以降を実行しているマルチサイトドメインの一部である場合にのみ、VRF 間サイト間 L3Out 設定でサポートされます。
- vzAny は、PBR でサービスグラフに関連付けられているコントラクトを、消費したり、または提供したりすることはできません。
- vzAny は、VRF 内通信を確立するためのコントラクトのプロバイダ、コンシューマ、または両方として設定できます。
- vzAny は、共有サービスのコンシューマとしてのみサポートされていますが、プロバイダとしてはサポートされていません。
- VzAny VRF は、EPG とそれを使用する BD を導入する予定のすべてのサイトに拡張することをお勧めします。
- APIC から既存の vzAny 設定をインポートできます。



(注) 既存の問題 (CSCvt47568) が原因の特定の事例で、Multi-Site Orchestrator から再展開する前にインポートされた設定を変更した場合、APIC で一部の変更が正しく更新されない場合があります。これを回避するには、インポート後すぐに設定を再展開してから、変更を加えます。変更されていない設定を再展開すると、通常どおりに更新できるようになります。

- vzAny プロバイダとコンシューマには、アプリケーション EPG、L3Outs に関連付けられた外部 EPG、インバンドまたはアウトオブバンドアクセスのためのエンドポイントグループが含まれます。
- vzAny は、外部発信トラフィックの 0.0.0.0/0 分類を暗黙に作成し、任意の外部 IP サブネットから発信されたすべてのトラフィックを許可します。VzAny が VRF に使用されている場合は、その VRF の L3Outs 部分に関連付けられた外部 EPG も含まれているため、VRF 自体で指定されたサブネットを含む L3external 分類を作成したことに相当します。
- VRF 内の EPG が別の VRF の EPG から共有サービス コントラクトを消費している場合、プロバイダ VRF の EPG からのトラフィックは、コンシューマ VRF 内でフィルタリングされます。vzAny は、送信元または宛先 EPG のワイルドカードに相当します。

コンシューマ VRF の vzAny と別のプロバイダー VRF の EPG1 の間で共有サービス契約を設定する場合は注意してください。ポリシーの適用 (フィルタリング) は常にコンシューマ VRF で実行されるため、プロバイダー VRF の一部である別の EPG2 に関連付けられたサブネットがコンシューマ VRF に漏洩した場合、EPG2 は、明示的にコントラクトを提供しなくても、VRF 全体でコンシューマ EPG との通信を開始します。このガイドラインに従わないと、VRF にわたる EPG 間での意図しないトラフィックが発生する可能性があります。

- 「Allow all」フィルタを使用して、コントラクトのプロバイダとコンシューマの両方として vzAny を使用した VRF を設定することは、非強制 VRF の設定と同じです。これは、その VRF 内のすべての EPG がコントラクトなしで相互に通信できることを意味します。
- コントラクトの範囲がアプリケーションプロファイルの場合、vzAny 設定は無視され、フィルタルールが拡張されます。CAM 使用率は、特定のコントラクトがコンシューマとプロバイダ EPG の各ペアの間に展開された場合と同じです。この場合、TCAM スペースの使用には利点がありません。
- 共有サービスの場合は、コンシューマ (vzAny) 側の宛先の分類 (Pctag) を適切に導出するために、EPG の下にプロバイダ EPG 共有サブネットを定義する必要があります。コンシューマとプロバイダの両方のサブネットがブリッジドメイン下で定義され、共有サービス コンシューマとして機能する vzAny に対して、BD から BD への共有サービス設定から移行する場合は、少なくとも共有フラグを使用してプロバイダ サブネットを EPG に追加する追加の設定手順を実行する必要があります。ただし、EPG の下のサブネットは接続に必要なではないため、常に No default SVI gateway フラグをチェックすることを推奨します。

定義済みの BD サブネットの複製として EPG サブネットを追加する場合は、サブネットの両方の定義に同じフラグが定義されていることを確認してください。それをしない場合、エラーが発生する可能性があります。

コントラクトとフィルタの作成

vzAny を使用するときは、基本的にコントラクト関係の単一のポイントを作成します。そのため、そのような関係とコントラクトのフィルタに使用する一般的なコントラクトが必要です。

このセクションでは、特別にこの目的の新しいコントラクトを作成する方法を説明します。代わりに、各 APIC サイトで構成した既存のコントラクトのインポートを選択できます。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] を選択します。

ステップ 3 コントラクトを作成したいスキーマを選択します。

更新する既存のスキーマがある場合は、メインウィンドウペインでスキーマの名前をクリックするだけでかまいません。そうではない場合、新しいスキーマを作成する場合は、[スキーマの追加 (Add Schema)] ボタンをクリックして、いつも通り、名前やテナントなど、スキーマ情報を指定してください。

ステップ 4 フィルタを作成します。

- a) **フィルタ** エリアまでスクロールし、+ をクリックしてフィルタを作成します。
- b) コントラクトの名前を指定します。
- c) [+エントリ (+ Entry)] をクリックし、フィルタ エントリを追加します。
- d) [エントリの追加 (Add Entry)] ウィンドウでフィルタの詳細を入力します。

通常、許可するトラフィックの種類を定義する場合と同様に、フィルタの詳細を指定します。

- e) **[保存 (SAVE)]** をクリックして、エントリを追加します。
- f) (オプション) 必要な場合は、追加のフィルタ エントリを作成します。

ステップ5 コントラクトを作成します。

- a) **コントラクト** エリアまで下方へスクロールし、+ をクリックして新しいコントラクトを追加します。
- b) コントラクトの名前を指定します。

例: contract-vzany。

- c) コントラクトの範囲を選択します

使用例に適切な範囲を選択します。たとえば、クロステナント共有サービスを有効にする場合は、範囲を「グローバル (Global)」に設定します。

- d) コントラクトが両方向に適用されるかどうかを選択します。
- e) **[+フィルタ (+Filter)]** をクリックして、1つ以上のコントラクト フィルタを追加します。
- f) **[フィルタ チェーンの追加 (Add Filter Chain)]** ウィンドウで、前の手順で作成されたフィルタを選択します。
- g) **[保存 (SAVE)]** をクリックして、フィルタを追加します。
- h) (オプション) 必要な場合は、手順を繰り返してフィルタを追加します。
- i) (オプション) **[両方向を適用 (Apply Both Directions)]** オプションを無効にする場合、コンシューマーとプロバイダの両方向にフィルタを提供します。

これで、次のセクションの vzAny で使用するコントラクトを作成しました。

コントラクトを消費または提供するための vzAny の設定

ここでは、vzAny VRF を作成する方法、または vzAny の既存の VRF を有効にする方法について説明します。

始める前に

次のものがが必要です。

- [コントラクトとフィルタの作成 \(340 ページ\)](#) の説明に従って、vzAny で使用するコントラクトと1つ以上のフィルタを作成しました。

ステップ1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ3 VRF の定義を持つ特定のテンプレートを含むスキーマを選択します。

新しい設定の場合、**[スキーマの追加 (Add Schema)]** ボタンを使用して新しいスキーマを作成し、VRF を設定できる新しいテンプレート (対象のテナントに関連付けられている) を定義できます。

ステップ4 VRF を作成または選択します。

コントラクトを提供または消費するために vzAny を設定する既存の VRF がある場合は、メイン ウィンドウ ペインで [VRF] をクリックします。それ以外の場合は、新しい VRF を作成する場合、[VRF] エリアまで下にスクロールし、[+] 記号をクリックします。

ステップ 5 [vzAny] を選択します。

右側のサイドバーで、[vzAny] チェックボックスをオンにします。

ステップ 6 vzAny コントラクトを選択します。

[+ Contract] オプションは、[vzAny] チェックボックスを有効にすると使用可能になります。

- a) [+コントラクト (+Contract)] をクリックし、新しいコントラクトを追加します。
- b) コントラクトを選択します。

[コントラクトとフィルタの作成 \(340 ページ\)](#) で作成したコントラクトを選択します。

- c) 契約タイプを選択します。

使用例に基づいて、契約のコンシューマまたはプロバイダのいずれかを選択できます。

vzAny VRF の一部として EPG を作成する

VzAny のユースケースには、新規作成するか、既存の EPG を使用するかを選択できます。EPG に明示的な vzAny 設定はなく、EPG が VRF の BD に関連付けられるとすぐに、EPG はその VRF (vzAny VRF) の vzAny 論理グループの一部になります。すでに作成され、構成されているすべての EPG に対して vzAny を有効にしているだけである場合は、このセクションをスキップすることができます。

始める前に

次のものがが必要です。

- [コントラクトとフィルタの作成 \(340 ページ\)](#) の説明に従って、vzAny で使用するコントラクトと1つ以上のフィルタを作成しました。
- [コントラクトを消費または提供するための vzAny の設定 \(341 ページ\)](#) の説明に従って、vzAny VRF を作成してコントラクトに割り当てました。

ステップ 1 vzAny VRF の一部として EPG を作成する場合

- a) EPG に使用する BD を作成してください。
- b) BD 構成サイドバーの [Virtual Routing & Forwarding (仮想ルーティングと転送)] ドロップダウンで、作成する vzAny VRF を選択します。
- c) EPG を作成します。

- d) EPG 設定サイドバーの [**Bridge Domain(ブリッジドメイン)**] ドロップダウンでは、作成する BD を選択します。

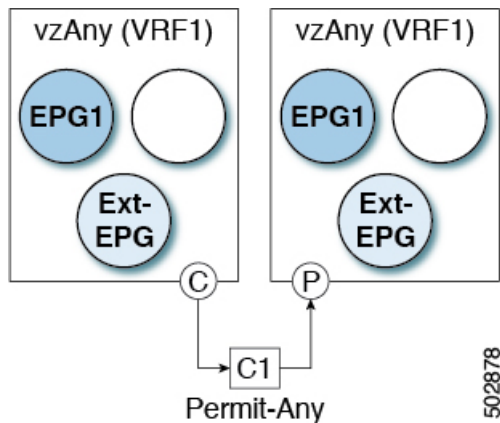
ステップ 2 vzAny VRF の一部として外部 EPG を作成する場合

- a) 外部 EPG を作成します。
b) 外部 EPG 構成サイドバーの [**Virtual Routing & Forwarding (仮想ルーティングと転送)**] ドロップダウンで、作成する vzAny VRF を選択します。

自由な VRF 間通信

このセクションでは、制限の課されない VRF 間通信のための、様々なスキーマの例を示します。示されているすべてのシナリオにおいて、vzAny は `permit any` フィルタを使用してコントラクトを提供し、消費します。これは基本的に、ポリシーを適用せずに ACI ファブリックをネットワーク接続にのみ使用します。これは、VRF 非強制 オプションと同等です。

図 41:



次のすべての使用例では、以下で要約されているものと同じ目的とポリシーを作成する必要があります。ただし、スキーマとテンプレート設計は、サイトの数だけではなく、拡大するオブジェクトに応じて異なります。以下の特定のセクションには、テンプレートレイアウトに関する推奨事項が含まれます。

ステップ 1 スキーマを作成します。

ステップ 2 すべてのサイトにあるオブジェクトの構成を展開するために使用する共通のテンプレートを作成します（つまり *stretched objects*）。

ステップ 3 EPG が展開されるサイトのそれぞれの組み合わせに対して、追加のテンプレートを作成します。

1つのテンプレートをすべてのサイトに展開する場合は、この手順をスキップできます。このセクションの使用例のダイアグラムは、テンプレートの例を示します。

ステップ 4 共通テンプレート内で、vzAny によって消費/提供されるコントラクトとフィルタを作成します。

この特定の使用例では、コントラクトに 1 つの「permit-any」フィルタルールが必要です。

具体的な手順については、[コントラクトとフィルタの作成 \(340 ページ\)](#) を参照してください。

ステップ 5 共通テンプレート内で、VRF を作成し、「permit-any」ルールを使用して以前に定義されたコントラクトを消費して提供するように vzAny を設定します。

これにより、VRF 内の自由な通信を確立できるようになります。

具体的な手順については、[コントラクトを消費または提供するための vzAny の設定 \(341 ページ\)](#) を参照してください。

ステップ 6 各サイトのテンプレート内で、そのサイトにのみ展開される EPG を作成して設定します。

すべてのサイトに単一のテンプレートを展開する場合は、代わりに VRF と同じテンプレート内で EPG を作成します。このセクションの使用例のダイアグラムは、テンプレートの例を示します。

これについては、[vzAny VRF の一部として EPG を作成する \(342 ページ\)](#) で説明します。

ステップ 7 すべてのサイトに共通のテンプレートを割り当てます。

ステップ 8 各テンプレートを適切なサイトに割り当てます。

ステップ 9 テンプレートを展開します。

拡張された EPG

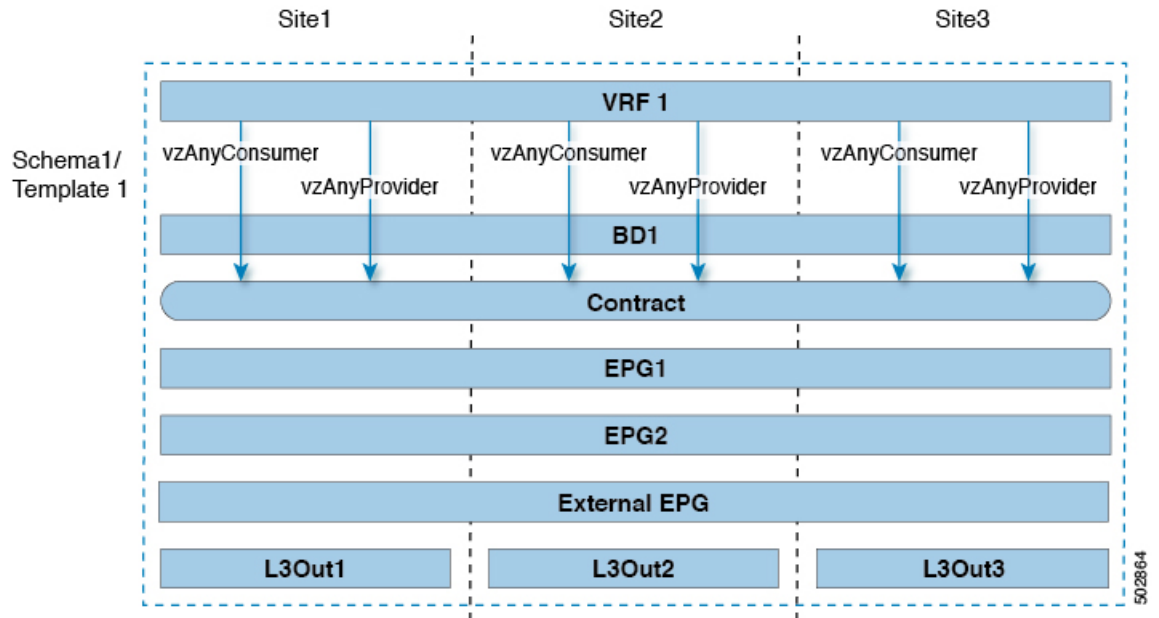
次の例は、EPG または外部 EPG の VRF 内通信を示し、それらのすべてはサイト間で拡張できます。この例では、EPG1 と EPG2 は同じ BD1 にマップされますが、両方の BD が VRF1 の一部である限り、それぞれが異なる BD の一部となる可能性があります。

このケースでは、同じテンプレート内のすべてのオブジェクトを作成し、テンプレートをすべてのサイトに展開できます。



(注) ベストプラクティスとして、代わりに L3Out オブジェクトを Cisco APIC でのみ定義したままにするか、MSO でオンサイト ローカル テンプレートを設定することをお勧めします。

図 42:



サイトローカル EPG

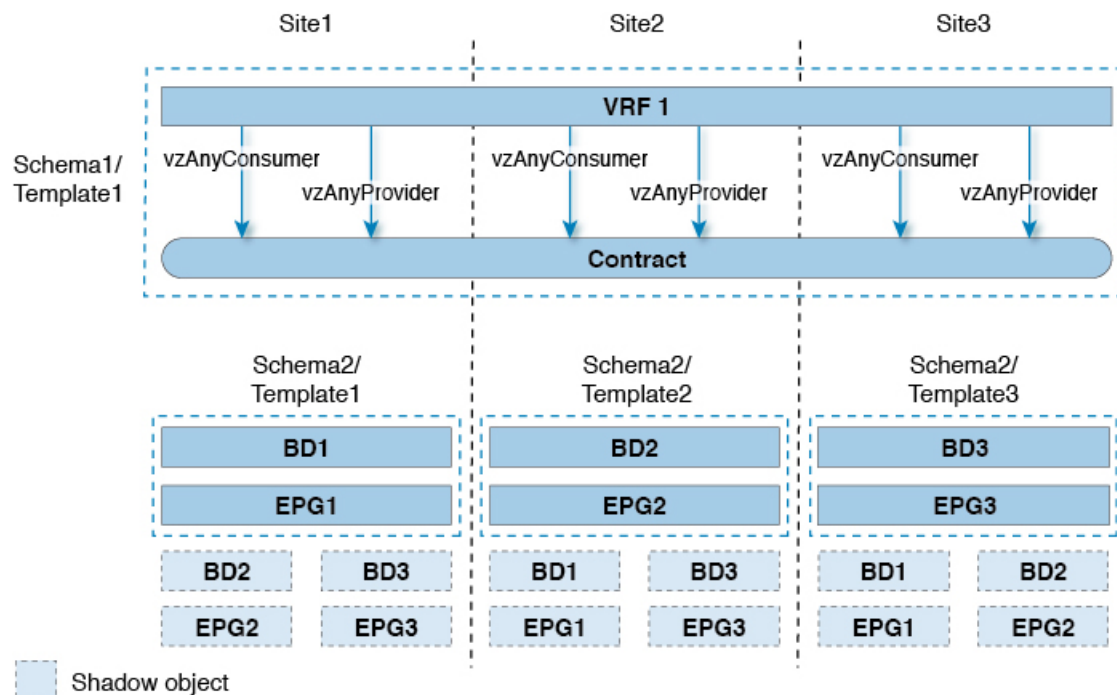
以下の例は、EPG または 外部 EPG 間の VRF 内通信を示しています。この場合、どの EPG も拡張されていませんが、vzAnyが「permit-any」コントラクトを消費して提供するため、相互に自由に通信できます。

この場合、複数のテンプレートを作成する必要があります。

- 各サイトに展開された共有オブジェクト (VRF、コントラクト) の単一のテンプレート。
- およびそのサイトに展開された EPG と BD を含むサイトごとの個別のテンプレート。

拡張されていないオブジェクトの場合は、シャドウオブジェクトがほかのサイトで作成されます。

図 43:



502865

サイト ローカルおよび拡張 EPG の組み合わせ

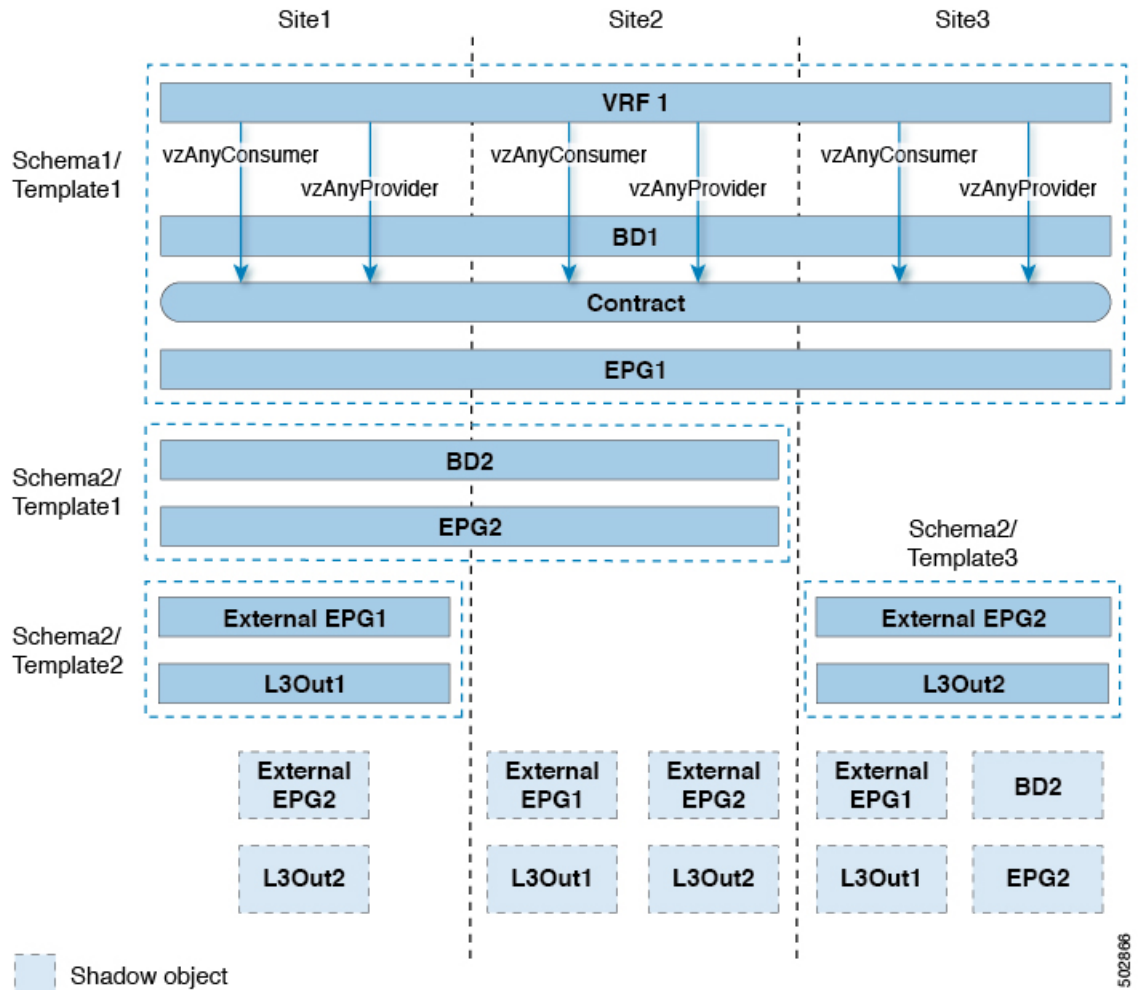
次の例は、EPG または 外部 EPG の間の VRF 内通信を示しています。一部の EPG は拡張されていますが、他のものは単一のサイトにのみ展開されます。それでも、すべての EPG は相互に自由に通信できます。vzAny は「すべて許可」のコントラクトを消費し、提供するからです。

この場合、複数のテンプレートを作成する必要があります。

- すべてのサイトに展開されている共有オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレート。
- また、これらのサイトにのみ展開されたオブジェクトを含むサイトの組み合わせごとに個別のテンプレートがあります。

拡張されていないオブジェクトの場合は、シャドウオブジェクトがほかのサイトで作成されません。

図 44:



502866

VRF 内のサイト間 L3Out

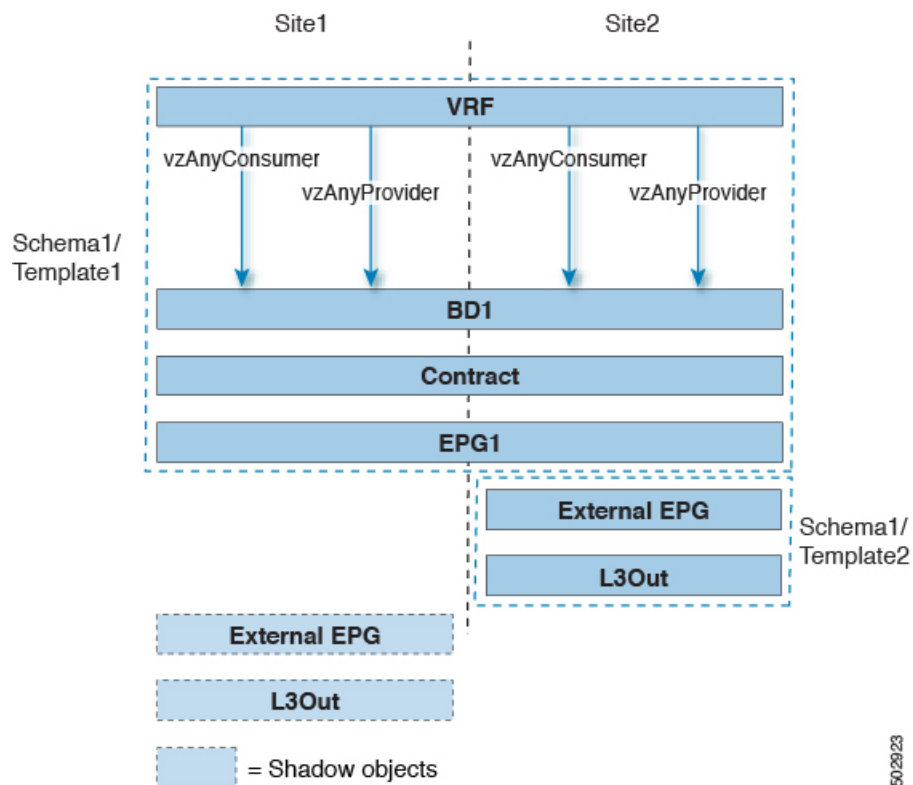
このユースケースでは、1つの vzAny VRF 内の複数の EPG 用に、サイト間 L3Out を設定できます。L3Out の外部 EPG が同じ VRF 内に存在する場合には、外部 EPG にプロバイダを明示的に追加する必要はありません。

この点を念頭に置くと、サイト間 L3Out を設定する場合には、ポッドごとにルーティング可能な TEP を設定することが必要になります。追加のサイト間 L3Out の詳細と要件については、[サイト間 L3Out の概要 \(215 ページ\)](#) のセクションで説明されています。

この場合、次のように、複数のテンプレートを作成する必要があります。

- まず、1つまたは複数のサイトに展開されている共有 vzAny オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレートです。
- また、これらのサイトにのみ展開されたオブジェクトを含む、サイトの組み合わせごとの個別のテンプレートです。

図 45:



上の図に示す構成に基づいて、拡張された EPG1 の一部であり、Site1 に接続されているエンドポイントは、Site2 に展開された L3Out 接続を介して外部ネットワークドメインと通信できます。同じことが、サイト 1 に展開されたサイトローカル EPG の一部であるエンドポイントにも当てはまります。

VRF 間 サイト間 L3Out

この使用例では、コンシューマー VRF と別のプロバイダー VRF の L3Out 外部 EPG との間の vzAny コントラクトを有効にすることができます。vzAny コンシューマー VRF の一部である複数の EPG は、提供 VRF で共有サービスを提供している単一の EPG と通信できます。vzAny 契約は、VRF 内のすべての EPG の契約として機能します。参加している各 VRF および L3Out 外部 EPG は、サイト全体に拡張できます。



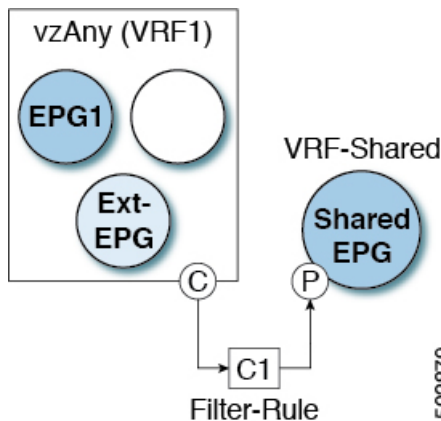
(注) VRF を vzAny プロバイダーにすることはできません。

多対1の通信

以下の3つのセクションでは、共有サービスを提供する単一の EPG との同じ vzAny VRF 通信の一部である、複数の EPG のスキーマの例を示します。この例では、1つ以上のフィルタルールを指定できます。

共有サービスを提供する EPG は、個別の VRF 内のものであることも (下の図を参照)、vzAny VRF の一部であることも可能です。

図 46:



次のすべての使用例では、以下で要約されているものと同じ目的とポリシーを作成する必要があります。ただし、スキーマとテンプレート設計は、サイトの数だけではなく、拡大するオブジェクトに応じて異なります。以下の特定のセクションには、テンプレートレイアウトに関する推奨事項が含まれます。

-
- ステップ 1** スキーマを作成します。
 - ステップ 2** すべてのサイトにあるオブジェクトの構成を展開するために使用する共通のテンプレートを作成します (つまり *stretched objects*) 。
 - ステップ 3** EPG が展開されるサイトのそれぞれの組み合わせに対して、追加のテンプレートを作成します。
 - ステップ 4** 共通テンプレート内で、vzAny によって消費され、共有サービスを提供する EPG によって提供される、コントラクトとフィルタを作成します。
これについては、[コントラクトとフィルタの作成 \(340 ページ\)](#) で説明します。
 - ステップ 5** 共通テンプレート内で、VRF を作成し、前に定義したコントラクトを消費してするよう vzAny を設定します。
これについては、[コントラクトを消費または提供するための vzAny の設定 \(341 ページ\)](#) で説明します。
 - ステップ 6** 各サイトのテンプレート内で、vzAny VRF の一部となる EPG を作成して設定します。
これについては、[vzAny VRF の一部として EPG を作成する \(342 ページ\)](#) で説明します。

ステップ7 プロバイダ EPG を新規作成して設定するか、既存のプロバイダ EPG または外部 EPG を設定します。

プロバイダ EPG の新規作成と設定、既存のプロバイダ EPG または外部 EPG の設定は、通常どおりの方法で行います。

ステップ8 プロバイダ EPG にコントラクトを割り当てます。

vzAny が消費するコントラクトの割り当てに加えて、同じコントラクトをプロバイダ EPG に割り当てることも必要になります。

VzAny VRF 内のプロバイダ EPG

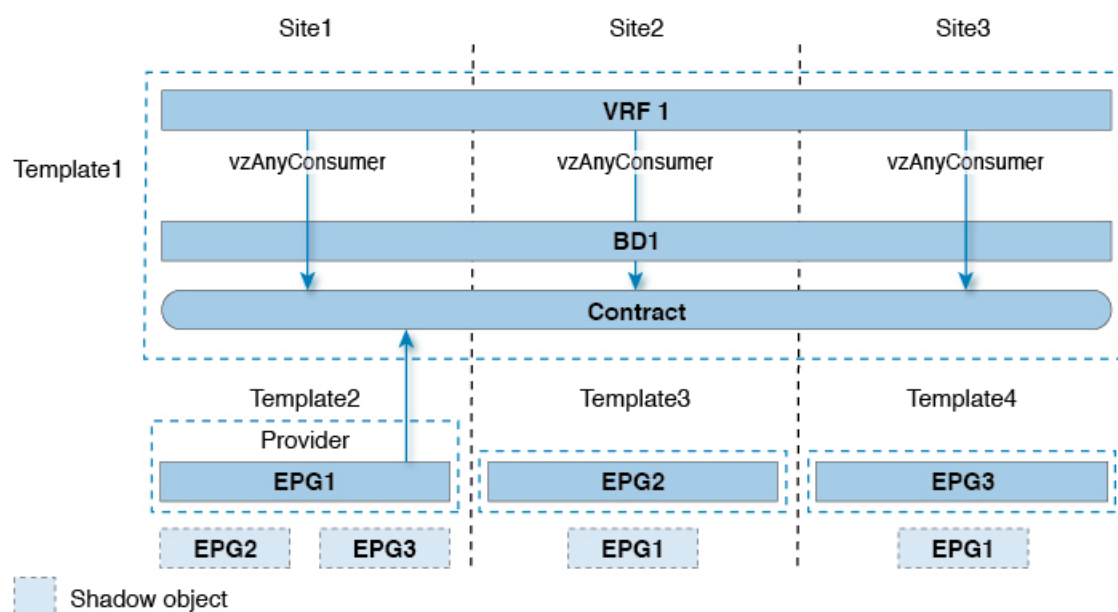
次の例は、単一のプロバイダ EPG (たとえば、共有サービス) と、同じ VRF 内の他のすべての EPG 間のサービスを消費する VRF 間の通信を示しています。

この場合、複数のテンプレートを作成する必要があります。

- すべてのサイトに展開されている共有オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレート。
- また、これらのサイトにのみ展開されたオブジェクトを含むサイトの組み合わせごとに個別のテンプレートがあります。

次の図は、1つのストレッチ VRF/BD の設定を示しています。代わりに、EPG ごとに専用 BD を設定してマッピングすることもできます。その場合は、シャドウ BD がリモートサイトに展開されます。

図 47:



502867

独自の VRF でのプロバイダ EPG

次の例は、独自の VRF 内の単一の EPG (たとえば、共有サービスプロバイダ) と、異なる vzAny VRF 内のすべての EPG との間の通信を示しています。プロバイダ EPG は、vzAny VRF のコンシューマ EPG と同じサイトまたは別のサイトに展開できます。

この場合、次のように、複数のテンプレートを作成する必要があります。

- まず、1 つまたは複数のサイトに展開されている共有 vzAny オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレートです。
- また、これらのサイトにのみ展開されたオブジェクトを含む、サイトの組み合わせごとの個別のテンプレートです。

図 48:

