



Cisco ACI マルチサイト コンフィギュレーションガイド、リリース 2.1 (x)

初版：2019年1月27日

最終更新：2019年1月28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 IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2019 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

[はじめに](#) ix

[表記法](#) ix

[関連資料](#) xi

[マニュアルに関するフィードバック](#) xi

[マニュアルの入手方法およびテクニカル サポート](#) xi

第 1 章

[新機能および変更された機能に関する情報](#) 1

[新機能および変更された機能に関する情報](#) 1

第 2 章

[GUI の概要](#) 3

[Cisco ACI マルチサイト Orchestrator GUI の概要](#) 3

[ダッシュボード](#) 4

[サイト ページ](#) 7

[スキーマ ページ](#) 9

[\[Tenants\] ページ](#) 11

[ユーザ ページ](#) 13

[ポリシー ページ](#) 15

[管理ページ](#) 15

第 3 章

[インフラストラクチャ管理](#) 23

[Cisco ACI マルチサイト and Cisco APIC Interoperability Support](#) 23

[Cisco ACI マルチサイト 通信ポート](#) 24

[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](#) 25

[ファブリック アクセス グローバル ポリシーの設定](#) 25

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	27
リモート リーフ スイッチを含むサイトの設定	29
マルチサイト リモート リーフのガイドラインと制限事項	29
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	30
リモート リーフ スイッチの直接通信の有効化	30
サイトの追加	31
インフラの前提条件とガイドラインの設定	32
インフラの設定: 一般設定	33
サイト接続性情報の更新	33
インフラの設定: サイトの設定	34
インフラの設定: ポッドの設定	36
インフラの設定: スパイン スイッチ	36
インフラ設定の展開	37
マルチサイト Orchestrator GUI を使用したサイトの削除	38
Cisco ACI CloudSec 暗号化	38
CloudSec の要件とガイドライン	39
CloudSec 暗号化に関する用語	40
CloudSec の暗号化と復号の処理	41
CloudSec 暗号化キーの割り当てと配布	44
CloudSec 暗号化の Cisco APIC の設定	46
GUI を使用した CloudSec 暗号化の Cisco APIC の設定	47
NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定	48
REST API を使用した CloudSec 暗号化の Cisco APIC の設定	49
Cisco ACI マルチサイト Orchestrator GUI を使用した CloudSec 暗号化の有効化	49
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	50
NX OS スタイル CLI を使用したキー再生成プロセスの無効化と再有効化	51
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	51
Cisco APIC への マルチサイトのクロス起動	52
サイトから Cisco APIC をクロス起動する	52
スキーマからの Cisco APIC のクロス起動	53
プロパティ ペインから Cisco APIC をクロス起動する	53

Cisco ACI マルチサイトの管理対象オブジェクトを Cisco APIC GUI を使用して表示する。

54

第 4 章

テナント管理 57

テナント管理のガイドライン 57

テナントの追加 58

テナントまたは Vrf 間でグローバル契約の設定 59

マルチサイト GUI を使用した EPG 内分離の設定 60

マルチサイト GUI を使用した マイクロセグメント EPG の設定 61

Epg を使用して、ドメインに関連付け、マルチサイト GUI 63

統合ビューですべてのテナントを表示する 64

第 5 章

ユーザ管理 65

ユーザ、ロール、および権限 65

ユーザ管理上のガイドライン 67

ユーザの追加 67

ユーザの管理 68

第 6 章

スキーマ管理 71

スキーマ設計上の考慮事項 71

単一スキーマの展開 71

ネットワーク分離での複数スキーマ 73

オブジェクトの関係性に基づく複数スキーマ 74

使用例の Cisco Cloud APIC スキーマ設計 76

スキーマ テンプレートの作成 76

APIC サイトからのスキーマ要素のインポート 77

アプリケーション プロファイルの設定 77

テナントの VRF を設定する 79

ブリッジ ドメインの設定 79

コントラクトのフィルタの設定 80

コントラクトの設定 80

外部 EPG の設定	81
L3Out の設定	82
スキーマの表示	82
テンプレート間でのオブジェクトの移行	82
シャドウ EPG と BD	84
サイト内 L3Out	85
サイト内 L3Out のガイドラインと制約事項	85
ルーティング可能な TEP アドレスの設定	87
サイト間 L3Out および VRF の作成またはインポート	87
サイト間 L3Out を使用するための外部 EPG の設定	88
サイト間 L3Out のコントラクトの作成	90
アプリケーション EPG のサイト間 L3Out の設定	90
サイト間での中継 L3Out の設定	93
サイト間 L3Out による共有サービス	95
EPG 優先グループ	96
優先グループに対する EPG の設定	97
レイヤ 3 マルチキャスト	98
レイヤ 3 マルチキャストルーティング	99
Layer 3 マルチキャストに関するガイドラインと制限事項	100
レイヤ 3 マルチキャストの有効化	101

第 7 章

管理操作	103
サイトのステータスの表示	103
スキーマヘルスの表示	103
個々のサイトの障害の表示	104
DHCP リレーポリシー	105
注意事項と制約事項	105
DHCP リレーポリシーの作成	107
DHCP オプションポリシーの作成	108
DHCP ポリシーの割り当て	109
DHCP リレーコントラクトの作成	110

APIC での DHCP リレー ポリシーの確認	111
既存の DHCP ポリシーの編集または削除	112
システム ログ	113
トラブルシューティング レポートとログの生成	113
外部ログアナライザへのログ ストリーミングを有効にする	114
設定のバックアップと復元	115
バックアップと復元に関するガイドライン	116
リモート バックアップ	117
バックアップのリモートロケーションの設定	117
既存のバックアップをリモート ロケーションへ移動する	118
Adding an NFS Share to Store Backups	119
バックアップの作成	120
バックアップの復元	121
バックアップのダウンロード	122
バックアップのインポート	122
カスタム SSL 証明書	122
カスタム認証局の追加	123
カスタム キーリングの追加	123
カスタムキーリングのアクティブ化	124
カスタム証明書のトラブルシューティング	124
外部認証	125
外部認証サーバの設定に関するガイドライン	126
RADIUS または TACACS+ を認証プロバイダとして追加する	127
LDAP を認証プロバイダとして追加する	128
ログイン ドメインの作成	129
ログイン ドメインの編集、削除、または非アクティブ化	130
リモート ユーザのログイン	131
システム設定	131
システム エイリアスとバナー	131
ログイン試行回数とロックアウト時間	132
プロキシサーバ	133

第 8 章	Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理	135
	Cisco Cloud APIC と Cisco ACI マルチサイトについて	135
	Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加	136
	サイト間インフラストラクチャの設定	137
	Cisco Cloud APIC と ISN デバイス間の接続の有効化	138
	共有テナントの設定	142
	スキーマの作成	144
	アプリケーションプロファイルと EPG の設定	144
	ブリッジドメインの作成と VRF への関連付け	145
	コントラクトのフィルタの作成	146
	コントラクトの作成	146
	サイトをスキーマに追加する	147
	AWS でのインスタンスの設定	148
	エンドポイントセレクタの追加	150
	Cisco ACI Multi-Site 設定の検証	155



はじめに

この前書きは、次の項で構成されています。

- [表記法](#) (ix ページ)
- [関連資料](#) (xi ページ)
- [マニュアルに関するフィードバック](#) (xi ページ)
- [マニュアルの入手方法およびテクニカルサポート](#) (xi ページ)

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体を使用できない場合に使用されます。

表記法	説明
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体のスクリーンフォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



警告 安全上の重要な注意事項

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

SAVE THESE INSTRUCTIONS

関連資料

次のドキュメントには、Cisco ACI マルチサイト の追加情報が提供されます。

- *Cisco ACI* マルチサイト 基本ガイド
- *Cisco ACI* マルチサイト *Orchestrator* のインストールとアップグレード ガイド
- *Cisco ACI* マルチサイト コンフィギュレーション ガイド
- *Cisco ACI* マルチサイト *REST API* コンフィギュレーションガイド
- *Cisco ACI* マルチサイト トラブルシューティング ガイド

これらすべてのドキュメントは、次の URL で入手できます。 <http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしく願いたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、Cisco バグ検索ツール (BST) の使用法、テクニカル サポートの依頼方法、および追加情報の収集方法については、『*What's New in Cisco Product Documentation*』 (<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>) を参照してください。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに直接配信することもできます。RSS フィードは無料のサービスです。



第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの主な変更点の概要を示したものです。ただし、このリリースまでのこのガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。

表 1: 新機能および変更された機能に関する情報

Cisco ACI マルチサイトのバージョン	機能	説明	参照先
2.2(3)	プロキシ設定	プロキシサーバは、クラウドサイトへのマルチサイト Orchestrator 接続に対して設定して有効にすることができます。	詳細については、 プロキシサーバ (133 ページ) を参照してください。
2.2(1)	Cisco ACI マルチサイトおよび Cisco APIC の相互運用性サポート	複数のサイト Orchestrator と APIC の異なるリリースバージョンを同じ環境内で機能させるために、混合操作サポートが追加されました。	詳細については、 DHCP リレーポリシー (105 ページ) を参照してください。

Cisco ACI マルチサイトのバージョン	機能	説明	参照先
2.2(1)	スキーマとテンプレート間のオブジェクトの移行	ブリッジドメインと EPGs を同じまたは異なるスキーマ内のテンプレート間で移動できるようになりました。	詳細については、 テンプレート間でのオブジェクトの移行 (82 ページ) を参照してください。
2.2(1)	サイト間 L3Out	サイトは別のサイトの L3Out を使用できません。	詳細については、 サイト内 L3Out (85 ページ) を参照してください。
2.2(1)	DHCP リレー	1つの EPG 内のエンドポイントに対して DHCP リレーを設定して、別の EPG または外部 EPG の DHCP サーバにアクセスすることができます。	詳細については、 DHCP リレーポリシー (105 ページ) を参照してください。
2.2(1)	リモートバックアップ	リモートバックアップの場所は、Orchestrator GUI で設定できます。	詳細については、「 リモートバックアップ (117 ページ) 」を参照してください。



第 2 章

GUI の概要

- [Cisco ACI マルチサイト Orchestrator GUI の概要 \(3 ページ\)](#)
- [ダッシュボード \(4 ページ\)](#)
- [サイト ページ \(7 ページ\)](#)
- [スキーマ ページ \(9 ページ\)](#)
- [\[Tenants\] ページ \(11 ページ\)](#)
- [ユーザ ページ \(13 ページ\)](#)
- [ポリシー ページ \(15 ページ\)](#)
- [管理 ページ \(15 ページ\)](#)

Cisco ACI マルチサイト Orchestrator GUI の概要

Cisco ACI マルチサイト (マルチサイト) Orchestrator 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 ACI、APIC、およびクラウド APIC の実装を設定し、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 マルチサイト Orchestrator GUI ページの機能について、次のセクションで説明されています。

- [ダッシュボード \(4 ページ\)](#)
- [サイト ページ \(7 ページ\)](#)
- [スキーマ ページ \(9 ページ\)](#)
- [\[Tenants\] ページ \(11 ページ\)](#)
- [ユーザ ページ \(13 ページ\)](#)
- [ポリシー ページ \(15 ページ\)](#)

- [管理ページ \(15 ページ\)](#)

各ページの上部には、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)] メニューは、サイトまたはスキーマの追加、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、システムログ、および Swagger API ドキュメントなど、Multi-Site Orchestrator に関する概要情報にアクセスできます。

- このリリースの最新情報をクリックすると、お使いのリリースの新機能の概要と、その他のマルチサイトドキュメントへのリンクが表示されます。
- **[システムログ (System Logs)]** リンクをクリックすると、システムイベントログを設定およびダウンロードできます。詳細については、このガイドの「管理操作」の章を参照してください。
- **[Swagger ドキュメントの表示 (View Swagger 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。

[ユーザ (User)] アイコンを使用すると、パスワードの更新、設定、ブックマークなど、現在ログインしているユーザ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。

- **[パスワードのリセット (Reset Password)]** リンクを使用すると、現在ログインしているユーザのパスワードを更新できます。
- **[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。

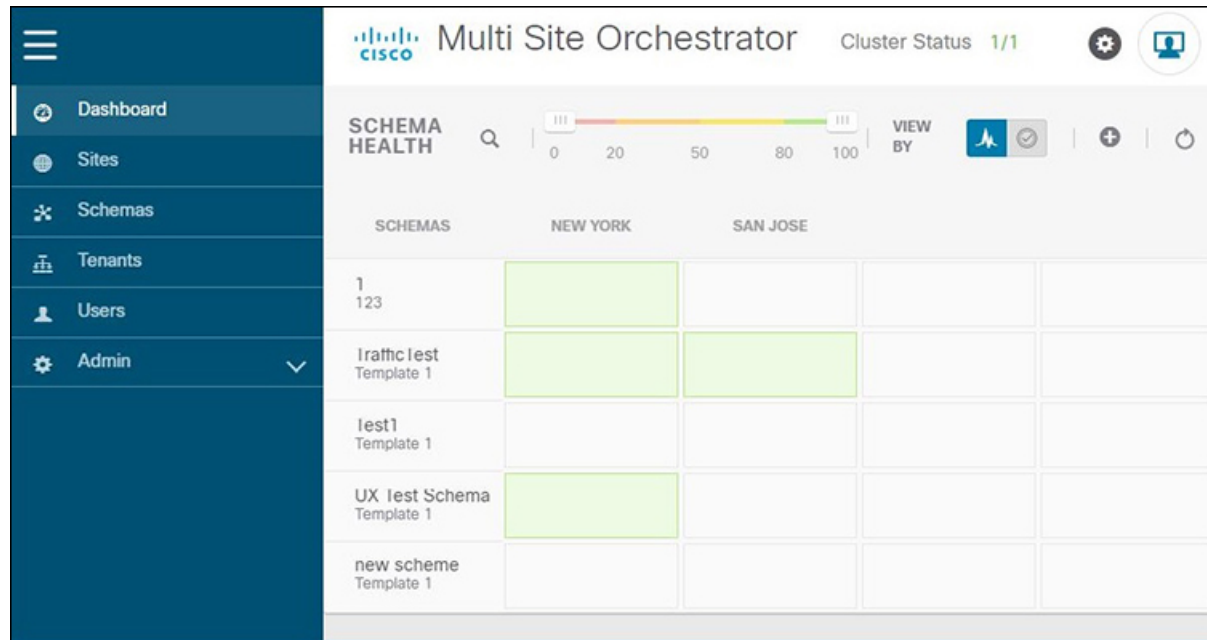
ファブリックオブジェクトを使用すると、オブジェクトが表示されるたびに、Orchestrator の GUI 全体で **[表示名 (Display Name)]** フィールドが使用されます。オブジェクトの作成時に表示名を指定できますが、Cisco APIC でのオブジェクトの命名要件により、無効な文字は削除され、結果の**内部名**はオブジェクトをサイトにプッシュするときに使用されます。テナントの作成時に使用される**内部名**は、通常、**[表示名 (Display Name)]** テキストボックスの下に表示されます。

ダッシュボード

マルチサイト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。

次のスクリーンショットは、マルチサイトダッシュボードの表示内容を示しています:

図 1: マルチサイトダッシュボード



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す。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。この機能は、Cisco ACI マルチサイト、リリース 1.0(2) から利用できるようになりました。

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、ACIマルチサイトは、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。ACIマルチサイトは、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なるためです。

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。

- **+ Add Site:** 当社の実装に別のサイトを追加できるようにします。+ **Add Site** をクリックした場合には、**Connection Settings** ページで、次のようなサイトについての詳細情報を入力する必要があります:

- **Name:** サイトの名前
- **Labels:** サイトのラベル ID。サイトには複数のラベルを関連付けることができます。
- **APIC Controller URL:** クラスターの識別用 URL には、さらに多くの APIC コントローラを追加することができます。
- **Username** と **Password:** admin レベルの権限を持つ APIC ログイン情報。
- **Specify Domain For Site:** デフォルトの認証ドメインが APIC 内で構成されている場合には、クリックしてスイッチをオンにし、ドメイン名を入力します。

新しいサイトの書齋を入力したら、**Save** ボタンをクリックします。

- **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。
- **+ Add Schema** をクリックして、サイトに新しいスキーマを追加するための手順を開始します。
- 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、**Schema Health** テーブルのサイト ロケールをクリックします。

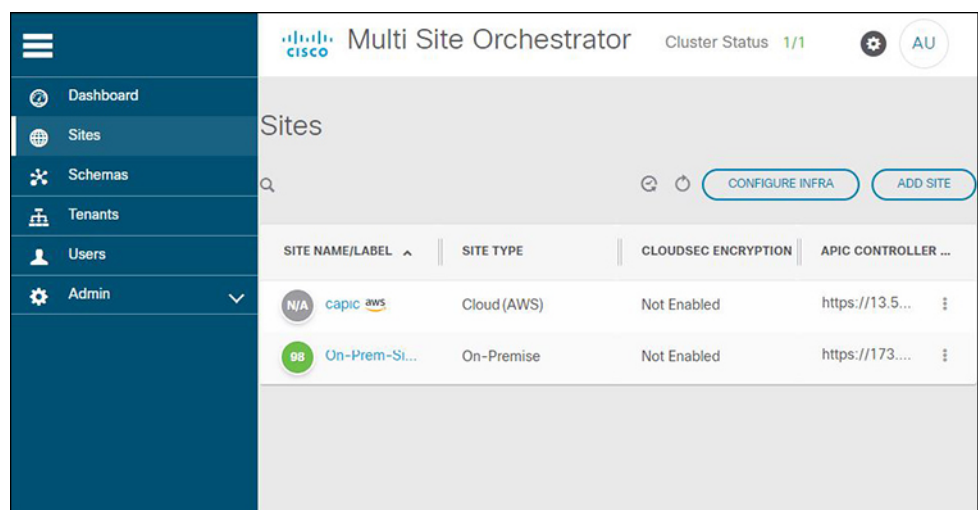
Schema Health テーブルはヒートマップタイプの表示になっています。対象としているスキーマの健全性が、色に従って表示されます。2つのカラム(つまり、ロケール)にまたがっているスキーマは、拡大状態であることを示しています。

- 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。

サイト ページ

マルチサイト [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。[Sites] ページの例が次のスクリーンショットに示されています。

図 2: マルチサイトの [Sites] ページ



[Sites] ページは次の2つのペインで構成されています:

- **[サイト名またはラベル (Site Name or Label)]**: サイトのステータスの表にはサイトの一覧が示されており、次のカラーコードによる識別子に従って、実装の現在のヘルスステータスが示されています:

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

特定のサイトをクリックすると、**[接続設定 (Connection Settings)]** 表示でサイトの詳細の確認や編集を行うことができます:

- **[名前 (Name)]**
- **[ラベル (Label)]**
- **[APIC コントローラ URL (APIC Controller URL)]**
- **[ユーザ名 (Username)]**と**[パスワード (Password)]**
- **[サイトのドメインの指定 (Specify Domain for Site)]**
- **[APIC サイト ID (APIC Site ID)]**

リストされているフィールドに変更を加えたら、**[保存 (Save)]** ボタンをクリックします。

- **[APIC コントローラ URL (APIC Controller URLs)]**: マルチサイト実装で関連付けられた APIC URL です。
- **[インフラの設定 (Configure Infra)]**: ファブリック インフラストラクチャの接続を設定するには、このエリアをクリックします。詳細については [Application Policy Infrastructure Controller \(APIC\)](#) ページを参照してください、。
- **[サイト追加 (Add Site)]**: 実装にサイトを追加するには、**[サイト追加 (Add Site)]** ボタンをクリックします。サイトを追加するには、次の詳細情報が必要です:
 - **[名前 (Name):]** サイト名です。
 - **[ラベル (Label):]** 既存のラベルを選択するか、新しいものを作成します。
 - **[APIC コントローラ URL (APIC Controller URL)]**: 既存の URL。新しい APIC コントローラ URL を追加するには、+ をクリックします。
 - **[ユーザ名 (Username)]**: サイトのユーザ名です。
 - **[パスワード (Password)]**: アクセスするための一意のサイト パスワードです。

- **[サイトのドメインの指定 (Specify Domain for Site)]**: サイトのドメインを指定するには、セレクトをクリックして **[On]** にします。

- **[アクション (Actions)]**: APIC ユーザインターフェイスの情報カテゴリを編集、削除、または開くための、ドロップダウンメニューリストのオプションです。

監査ログ

ログの詳細を一覧表示するには、**[監査ログ (Audit Log)]** アイコン (**[インフラの設定 (Configure Infra)]** タブの横) をクリックします。**[監査ログ: サイト リスト (Audit Logs: Sites 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 (Date)
- 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)]**: 1人のユーザまたはすべてのユーザをクリックして **[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をフィルタ処理できます。
- **[アクション (Action)]**: アクションを選択します。たとえば作成済み、更新済み、または削除済みを選択して **[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をフィルタ処理できます。

スキーマ ページ

マルチサイトスキーマ 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。

次のスクリーンショットは、統計情報の例を示しています。

図 3: 複数サイトのスキーマ ページ



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、表形式で次の情報が表示されます。

- **[名前 (Name)]**: 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 (Templates)]**: 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。拡張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 (Tenants)]**: 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 (Actions)]**: 関連付けられるスキーマを持つ **[アクション (Action)]** 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)] ボタンをクリックして、実装のために新しいスキーマを追加します。スキーマの作成に関する詳細は、[スキーマ管理 \(71 ページ\)](#) で説明されています。

監査ログ

スキーマ ページのログの詳細が表示するには、**[監査ログ (Audit Log)]** アイコンをクリックします。これは **[スキーマの追加 (Add Schema)]** タブの横にあります。**[監査ログ: スキーマ リスト (Audit Logs: Schemas 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 (Date)
- 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10日から2017年11月14日の範囲を選択して、[適用 (Apply)] をクリックすれば、その機関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。

スキーマの作成の詳細については、[スキーマ管理 \(71 ページ\)](#) を参照してください。

[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。

次のスクリーンショットは設定例を示します:

図 4: 複数サイトのテナント ページ

NAME ^	DESCRIPTION	ASSIG...	ASSIG...	ASSIG...	CONSISTENCY SCHEDULER
CiscoLive		1	1	1	Set Sche... ⋮
Cloudonly		0	1	1	Set Sche... ⋮
common	Common tenant f...	2	1	0	Set Sche... ⋮

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

Audit Log アイコン (**Add Tenant** タブの隣) をクリックすると、[Tenants] ページのログの詳細を一覧表示できます。 **Audit Logs: Tenants List** ページが表示されます。

ページのテーブルには、以下の詳細が表示されます:

- 日付 (Date)
- 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10日から2017年11月14日の範囲を選択して、[**適用 (Apply)**] をクリックすれば、その機関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:

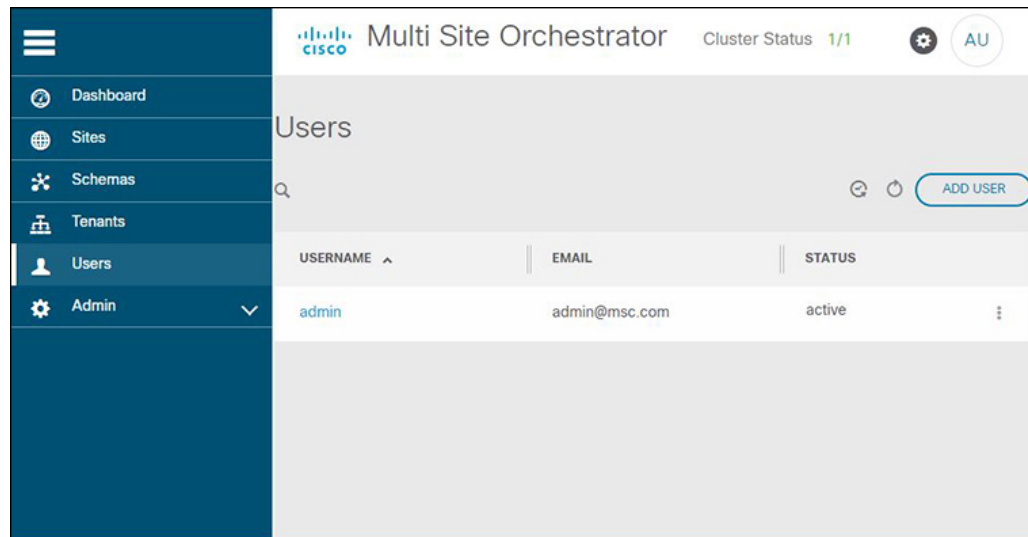
- [ユーザ (User)]: 1人のユーザまたはすべてのユーザをクリックして [**適用 (Apply)**] をクリックすると、ユーザ名に基づいてログの詳細をフィルタ処理できます。
- [アクション (Action)]: アクションを選択します。たとえば作成済み、更新済み、または削除済みを選択して [**適用 (Apply)**] をクリックすると、そのアクションに従ってログの詳細をフィルタ処理できます。

テナントの追加の詳細については、[テナント管理 \(57 ページ\)](#) を参照してください。

ユーザ ページ

マルチサイト Orchestrator の [**ユーザ (Users)**] ページにはすべてのユーザが表示されます。次に示すのは、[**ユーザ (Users)**] ページの例です。

図 5: [ユーザ (Users)] ページ



[ユーザ (Users)] ページには、ユーザ名および関連付けられている電子メールで識別されているすべてのユーザと、現在のアクティビティステータスの表が表示されます。[ユーザ名 (Username)] を選択してクリックすると、対象とするユーザに属する [一般設定 (General Setting)] ページが表示されます。[一般設定 (General Setting)] ページでは、ユーザ名、パスワード、電子メール、およびスイッチオンユーザロールなど、対象とするユーザに関連付けられている詳細を編集できます。

[ユーザの追加 (Add User)] をクリックすると、新しいユーザをマルチサイトの実装に追加できます。[一般設定 (General Setting)] ページの表示では、ユーザ名、パスワード、電子メール、スイッチオンユーザロールをマルチサイトの実装と関連付けることができます。

監査ログ

[ユーザ (Users)] ページのログの詳細を一覧表示するには、[監査ログ (Audit Log)] アイコン ([ユーザの追加 (Add User)] タブの隣) をクリックします。[監査ログ: ユーザリスト (Audit Logs: Users 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 (Date)
- 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10日から2017年11月14日の範囲を選択して、[適用 (Apply)] をクリックすれば、その機関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)]: 1 人のユーザまたはすべてのユーザをクリックして [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をフィルタ処理できます。
- [アクション (Action)]: アクションを選択します。たとえば作成済み、更新済み、または削除済みを選択して [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をフィルタ処理できます。

ポリシー ページ

マルチサイト 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。

使用可能なポリシータイプとその設定方法の詳細については、[管理操作 \(103 ページ\)](#) の章を参照してください。

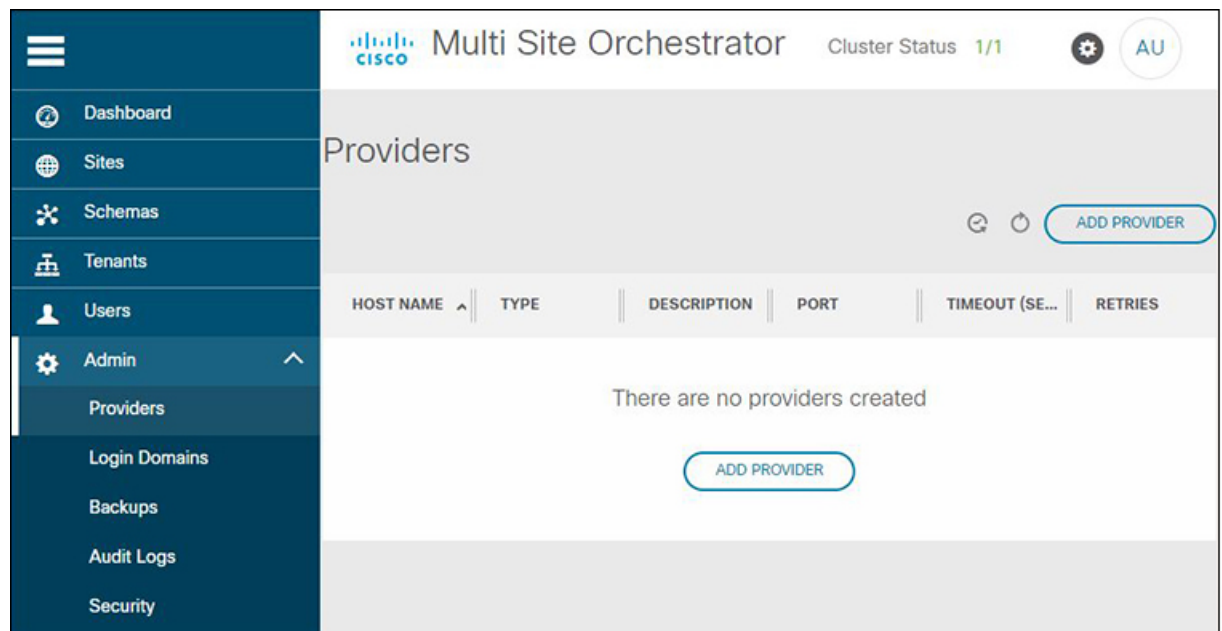
管理ページ

Cisco ACI マルチサイト Orchestrator ナビゲーションバーから [管理者 (Admin)] タブを選択すると、次の追加の管理ページが展開されます。

- プロバイダ
- ログイン ドメイン
- バックアップ
- 監査ログ
- セキュリティ
- リモート ロケーション
- システム設定

プロバイダ

図 6: Cisco ACI マルチサイト *Orchestrator* プロバイダ ページ



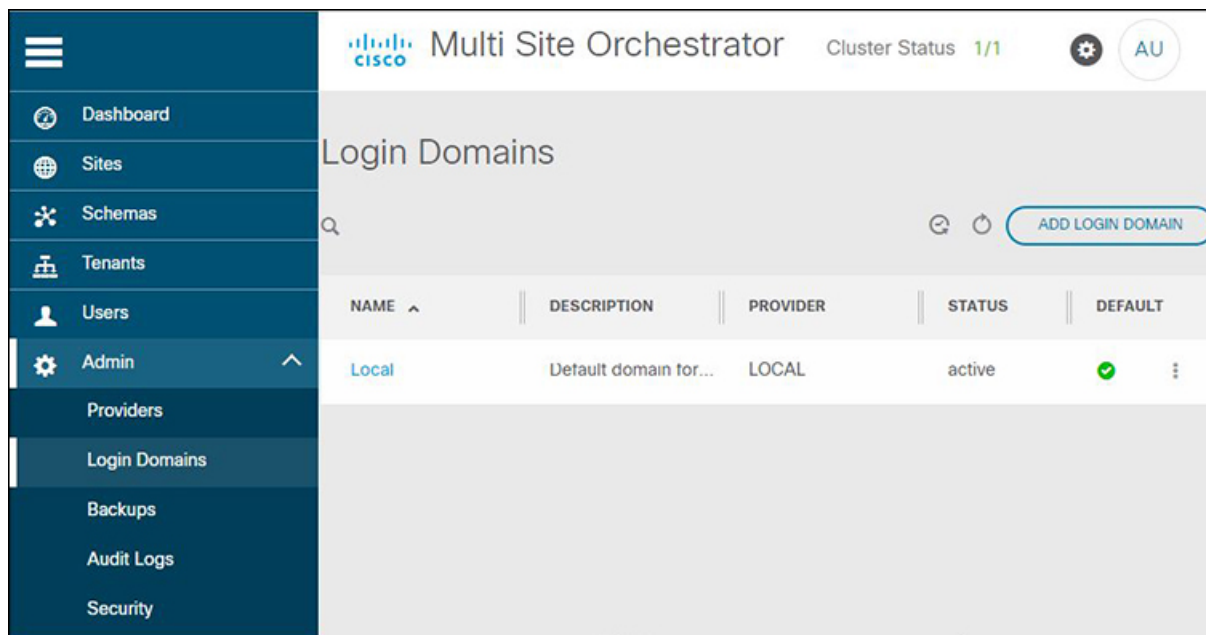
[管理 (Admin)] 見出しの下の [プロバイダ (Providers)] ページでは、設定された外部認証プロバイダに関する情報が表示されます。次の詳細が、各プロバイダに対して示されます。

- ホスト名
- タイプ
- 説明
- ポート
- タイムアウト (秒)
- リトライ

外部認証プロバイダの操作については、[管理操作 \(103 ページ\)](#) で説明しています。

ログイン ドメイン

図 7: Cisco ACI マルチサイト *Orchestrator* のログイン ドメイン ページ

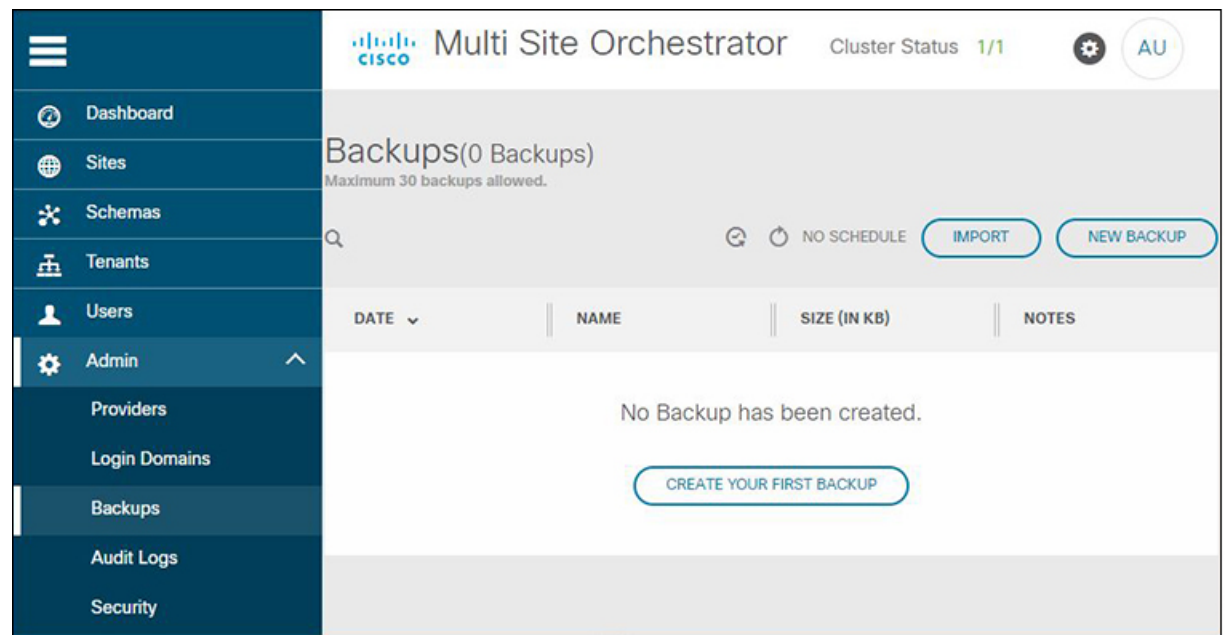


[管理 (Admin)] 見出しの下の [ログイン ドメイン (Login Domains)] ページでは、利用可能なログイン ドメインに関する情報が表示されます。各ドメインについて、次の詳細が表示されます。

- 名前
- 説明
- プロバイダ
- Status (ステータス)
- デフォルト (Default)

ログイン ドメインの操作については、[管理操作 \(103 ページ\)](#) で説明しています。

バックアップ

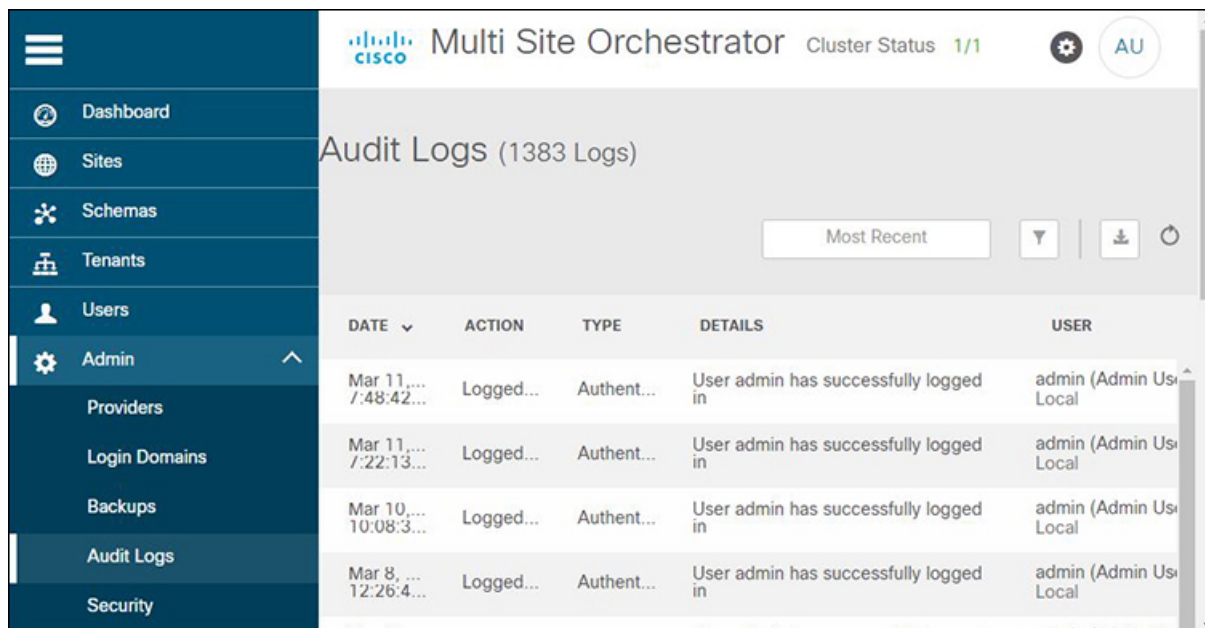
図 8: Cisco ACI マルチサイト *Orchestrator* のバックアップページ

[管理 (Admin)] 見出しの下の [バックアップ (Backups)] ページでは、作成したバックアップに関する情報が表示されます。次の詳細が、各ドメインに対して示されます。

- 日付
- 名前
- サイズ
- 注記

バックアップの操作については、[管理操作 \(103 ページ\)](#) で説明しています。

図 9: Cisco ACI マルチサイト Orchestrator 監査ログページ



The screenshot displays the 'Audit Logs (1383 Logs)' page in the Cisco ACI Multi Site Orchestrator. The left sidebar contains a navigation menu with options: Dashboard, Sites, Schemas, Tenants, Users, Admin (selected), Providers, Login Domains, Backups, Audit Logs, and Security. The main content area shows a table of audit logs with the following columns: DATE, ACTION, TYPE, DETAILS, and USER. The table lists several successful login events for the 'admin' user.

DATE	ACTION	TYPE	DETAILS	USER
Mar 11, 2017 7:48:42...	Logged...	Authent...	User admin has successfully logged in	admin (Admin User Local)
Mar 11, 2017 7:22:13...	Logged...	Authent...	User admin has successfully logged in	admin (Admin User Local)
Mar 10, 2017 10:08:3...	Logged...	Authent...	User admin has successfully logged in	admin (Admin User Local)
Mar 8, 2017 12:26:4...	Logged...	Authent...	User admin has successfully logged in	admin (Admin User Local)

監査ログ

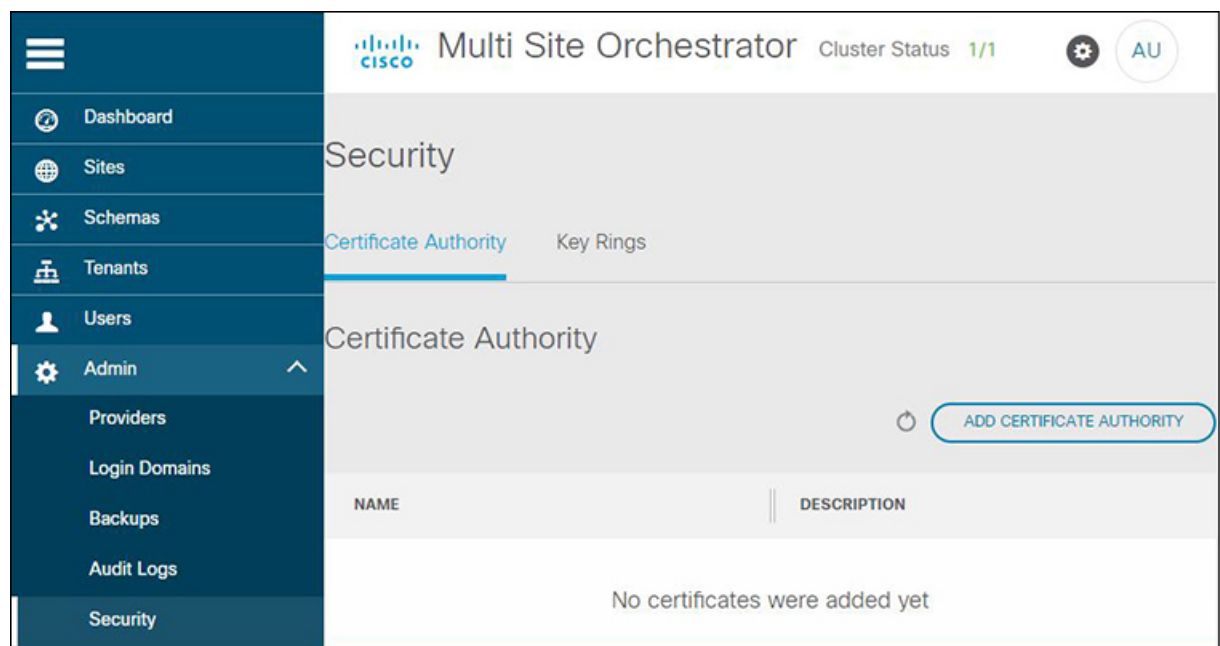
[管理 (Admin)] 見出しの下の [監査ログ (Audit Logs)] ページでは、監査ログとレコードに関する情報が占められます。次の詳細が表示されます。

- 日付 (Date)
- アクション
- タイプ
- 詳細
- ユーザ

ログの操作については、[管理操作 \(103 ページ\)](#) で説明しています。

セキュリティ

図 10: Cisco ACI マルチサイト *Orchestrator* セキュリティ ページ



[管理 (Admin)] 見出しの下の [セキュリティ (Security)] ページでは、Orchestrator により使用するために設定したカスタム証明書とキーリングに関する情報が示されます。次の詳細が示されます。

- 認証局
 - 名前
 - 説明
- キー リング
 - 名前
 - 説明
 - トラストポイント
 - 状態

証明書の操作は、[管理操作 \(103 ページ\)](#) で説明されています。

リモート ロケーション

[管理 (Admin)] 見出しの下の [リモート ロケーション (Remote Location)] ページでは、Orchestrator により使用するために設定したリモート バックアップ ロケーションに関する情報が表示されます。次の詳細が示されます。

- 名前

- ホスト
- プロトコル
- ユーザ名
- リモート パス

リモートバックアップの作業については、[管理操作（103 ページ）](#) で説明しています。

システム設定

[[管理 \(Admin\)](#)] 見出しの下の [[システム設定 \(System Configuration\)](#)] ページでは、Orchestrator GUIの動作方法を定義する多くのシステム設定を構成することができます。たとえば、失敗したログイン試行の処理方法を変更することや、GUIの上部に警告バナーを表示するかどうかを設定することができます。

使用可能なシステム設定の詳細については、[管理操作（103 ページ）](#) を参照してください。



第 3 章

インフラストラクチャ管理

- [Cisco ACI マルチサイト and Cisco APIC Interoperability Support](#) (23 ページ)
- [Cisco ACI マルチサイト 通信ポート](#) (24 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](#) (25 ページ)
- [リモート リーフ スイッチを含むサイトの設定](#) (29 ページ)
- [サイトの追加](#) (31 ページ)
- [インフラの前提条件とガイドラインの設定](#) (32 ページ)
- [マルチサイト Orchestrator GUI を使用したサイトの削除](#) (38 ページ)
- [Cisco ACI CloudSec 暗号化](#) (38 ページ)
- [Cisco APIC への マルチサイトのクロス起動](#) (52 ページ)

Cisco ACI マルチサイト and Cisco APIC Interoperability Support

リリース 2.2(1) より前では、すべてのサイトで同じ APIC バージョンを実行する必要があり、その APIC リリースに対応する Orchestrator のバージョンも実行する必要がありました。ファブリックのアップグレード中には、マルチサイト Orchestrator をアップグレードする前に、まずすべての APIC サイトをアップグレードする必要がありました。たとえば、APIC リリース 4.0(1) からリリース 4.1(1) にファブリックをアップグレードしている場合、すべてのサイトが APIC リリース 4.1(1) になるまで、Orchestrator のリリース 2.0 (1) を維持する必要がありました。

リリース 2.2(1) 以降では、マルチサイト Orchestrator リリースは APIC リリースから分離されています。各サイトと Orchestrator 自体の APIC クラスタは、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るようになりました。

混合操作モードは、次の APIC リリースのいずれかを実行しているサイトでサポートされています。

- 3.2(6) 以降
- 4.0(1) 以降
- 4.1(1) 以降

- 4.2(1) 以降

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 Orchestrator をアップグレードすると、新しい Orchestrator 機能が以前の APIC リリースでまだサポートされていない可能性があ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実行されます。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<サイトのバージョン>は、MSO ではサポートされていません。この<機能>に必要な最小バージョンは<必要なバージョン>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。

機能	最小バージョン
ACI マルチポッドのサポート	Release 3.2(1)
サービス グラフ (L4~L7 サービス)	リリース 3.2(1)
外部 EPG	リリース 3.2(1)
ACI 仮想エッジ VMM のサポート	リリース 3.2(1)
DHCP Support	リリース 3.2(1)
整合性チェッカー	リリース 3.2(1)
CloudSec 暗号化	リリース 4.0(1)
レイヤ 3 マルチキャスト	リリース 4.0(1)
OSPF の MD5 認証	リリース 4.0(1)
EPG 優先グループ	リリース 4.0(2)
ホストベースのルーティング	リリース 4.1(1)
サイト内 L3Out	リリース 4.2(1)

Cisco ACI マルチサイト 通信ポート

Cisco ACI マルチサイト 環境を設定する際は、下記のポートが Cisco ACI マルチサイト Orchestrator によって Cisco ACI マルチサイト 環境内のネットワーク通信に使用されることに注意してください。

Cisco ACI マルチサイト Orchestrator と Cisco APIC (サイト) 間のネットワーク通信に必要なポートは次のとおりです。

- TCP ポート 80/443 (APIC REST の設定展開用)

Cisco ACI マルチサイト Orchestrator ノード間のネットワーク通信に必要なポートは次のとおりです。

- TCP ポート 2377 (クラスタ管理通信用)
- TCP および UDP ポート 7946 (Manager 間の通信用)
- UDP ポート 4789 (Docker オーバーレイ ネットワーク トラフィック用)

Cisco ACI マルチサイト Orchestrator ノード間のすべてのコントロールプレーンおよびデータプレーントラフィックは、IP プロトコル番号 50 を使用して IPSec のカプセル化セキュリティペイロード (ESP) によって暗号化され、セキュリティを提供し、最大 150 ミリ秒の往復時間間隔でクラスタの展開を可能にします。いずれかの Orchestrator ノード間にファイアウォールがある場合は、このトラフィックを許可するために適切なルールを追加する必要があります。

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 Multi-Site Orchestrator に追加するか、Multi-Site Orchestrator により管理されるには、Multi-Site Orchestrator に追加する前に、各サイトで設定されなければならない多くのファブリック指定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、Multi-Site Orchestrator に追加および管理する前に、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 Multi-Site 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。

- a) 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。
- b) [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。

- a) 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 エントリー 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 Multi-Site Orchestrator から選択するものです。

- 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 \(27 ページ\)](#) 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 Multi-Site 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 \(25 ページ\)](#) 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 Profile)] 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。

- 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。
- [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 セクタ ポリシーを設定します。

- 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。
- [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、セレクトを保存します。
- 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、spine1-1SN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。

次のタスク

自分のサイトにリモートリーフスイッチが含まれる場合、[リモートリーフスイッチを含むサイトの設定 \(29 ページ\)](#) の説明に従って、ファブリック固有の設定をさらに変更する必要があります。

そうではない場合は、[サイトの追加 \(31 ページ\)](#) の説明に従って、Multi-Site Orchestrator へのサイト追加に進みます。

リモートリーフスイッチを含むサイトの設定

リリース 2.1 (2) 以降では、マルチサイトアーキテクチャはリモートリーフスイッチを使用する APIC サイトをサポートしています。ここでは、マルチサイト 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ガイドライン、制限事項、および設定手順について説明します。

マルチサイト リモートリーフのガイドラインと制限事項

マルチサイト 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 をリリース 4.1(2) 以降にアップグレードする必要があります。
- マルチサイト Orchestrator をリリース 2.1(2) 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、マルチサイト 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、]<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マルチサイト 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 (Routable Subnets)] 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 (Reserve Address Count)] を入力し、状態を[アクティブ (Active)] または [非アクティブ (Inactive)] 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マルチサイト 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、マルチサイト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。

- a) 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。
- b) 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。
- c) [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。

- d) [送信 (Submit)] をクリックして変更を保存します。

サイトの追加

このセクションでは、Cisco ACI マルチサイト Orchestrator GUI を使用してサイトを追加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、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。

ステップ1 マルチサイト GUI にログインし、[Main menu] で、[Sites] をクリックします。

初めてログインしている場合、**admin** ユーザとして、デフォルトパスワード **We1come2msc!** を使用してログインすると、デフォルトパスワードを変更するように指示するプロンプトが表示されます。新しいパスワードの要件は、次のとおりです。

- 最低 12 文字
- 最低 1 つの英字
- 最低 1 つの数字
- * およびスペースとは異なる、少なくとも 1 つの特殊文字

ステップ2 メインペインの右上にある [サイトの追加 (Add Site)] をクリックします。

ステップ3 [サイトの追加 (Add Site)] 画面で、サイトの詳細を指定します。

- a) [名前 (Name)] フィールドに、サイト名を入力します。

- b) **[ラベル (Labels)]** フィールドで、ラベルを選択するか作成します。
サイトに対して複数のラベルを指定することができます。
- c) **[APIC Controller URL]** フィールドに、Cisco APIC の URL を入力します。
APIC URL に対して、http または https プロトコルと IP アドレスまたは DNS ホスト名を使用できます。たとえば、https://<ip-address> または https://<dns-hostname> です。
- d) ファブリックの APIC のクラスタがある場合は、**[+APIC Controller URL]** をクリックして、追加の URL を指定します。
- e) **[ユーザ名]** フィールドに、サイトの APIC の管理者ユーザのユーザ名を入力します。
- f) **[パスワード]** フィールドに、ユーザのパスワードを入力します。
- g) サイトのドメイン名を指定する場合には、**[サイトのログイン ドメインの指定 (Specify Login Domain for Site)]** スイッチをオンにします。
このオプションをオンにした場合、**[ドメイン名]** フィールドにドメイン名を入力します。
- h) **[APIC サイト ID]** フィールドに、固有なサイト ID を入力します。
サイト ID は Cisco APIC サイトの固有識別子で、1~127 の範囲になければなりません。サイト ID が指定されると、サイト ID は Cisco APIC を工場出荷時にリセットせずに、変更できません。

ステップ 4 **[保存 (Save)]** をクリックして、サイトを追加します。

ステップ 5 プロンプトが表示されたら、プロキシ設定の更新を確認します。

プロキシサーバを使用するように Orchestrator を構成し、「プロキシなし」リストにまだ含まれていないオンプレミスサイトを追加する場合、Orchestrator はプロキシ設定の更新を通知します。

プロキシ設定の詳細については、『Cisco ACI Multi-Site 設定ガイド』の「管理オプション」の章を参照してください。

ステップ 6 サイトを追加するには、これらの手順を繰り返します。

インフラの前提条件とガイドラインの設定

次のセクションでは、全般な設定と、サイト固有の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。

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。これには、以下が含まれます。

- 各サイトのファブリック アクセス ポリシーの設定。
- リモートリーフスイッチを使用したサイトの直接通信およびルーティング可能なサブネットの設定。

さらに、次の点に注意してください。

- スパインスイッチまたはスパインノード ID の変更の追加や削除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 \(33 ページ\)](#) に記載されている マルチサイト ファブリック接続情報の更新が必要です。
- Orchestrator に割り当てられているオーバーレイ ユニキャスト TEP、オーバーレイ マルチキャスト TEP、および BGP EVPN ルータ ID IP 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。

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。

-
- ステップ 1** Cisco ACI マルチサイト Orchestrator GUI にログインします。
 - ステップ 2** [メインメニュー (Main menu)] で [サイト (Site)] をクリックします。
 - ステップ 3** [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] をクリックします。
 - ステップ 4** 左側のペインの [設定 (settings)] で、[一般設定 (General Settings)] をクリックします。
 - ステップ 5** [BGP ピアリング タイプ (BGP Peering Type)] ドロップダウンから、[フルメッシュ (full-mesh)] または [ルートリフレクタ (route-reflector)] のいずれかを選択します。

[ルートリフレクタ (route-reflector)] オプションは、すべてのサイトが同じ BGP 自律システム (AS) に属している場合にのみ有効です。
 - ステップ 6** [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。
 - ステップ 7** [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。
 - ステップ 8** [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。
 - ステップ 9** [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。
 - ステップ 10** [最大 AS 制限値 (Maximum AS Limit)] フィールドで、最大 AS 制限値を入力します。
 - ステップ 11** [ピア間 BGP TTL (BGP TTL Between Peer)] フィールドで、ピア間の BGP TTL を入力します。
-

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、マルチサイト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 ACI マルチサイト Orchestrator GUI にログインします。
 - ステップ 2 [メインメニュー (Main menu)] で [サイト (Site)] をクリックします。
 - ステップ 3 [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] 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簿宅をクリックします。
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: サイトの設定

ここでは、サイトごと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 ACI マルチサイト Orchestrator GUI にログインします。
 - ステップ 2 [メインメニュー (Main menu)] で [サイト (Site)] をクリックします。
 - ステップ 3 [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] 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 右側の [<サイト> 設定 (Settings)] ペインで、[ACI マルチサイト (ACI Multi-Site)] ノブを有効にして Orchestrator でサイトを管理できるようにします。
 - ステップ 6 (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 ACI Multi-Site Configuration Guide* の Infrastructure Management の章を参照してください。
 - ステップ 7 [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。
 - ステップ 8 [BGP 自律システム番号 (BGP Autonomous System Number)] を指定します。
 - ステップ 9 [BGP パスワード (BGP Password)] を指定します。
 - ステップ 10 [OSPF Area ID (OSPF エリア ID)] を指定します。
マルチサイト インフラ OSPF の詳細を設定するには、OSPF エリア 0 を使用することを推奨します。0 以外のエリア ID を使用する場合は、次の手順ではそれを regular OSPF エリア タイプとして設定することになります。 stub エリア タイプにはなりません。
 - ステップ 11 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。
OSPF エリアタイプは、次のいずれかになります。

- nssa

- regular
- stub

ステップ 12 ドロップダウンメニューから外部ルート ドメインを選択します。

APIC GUI で作成した外部ルータ ドメインを選択します。

ステップ 13 サイトの OSPF 設定を行います。

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。

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 ACI マルチサイト Orchestrator GUI にログインします。

ステップ2 [メインメニュー (Main menu)]で [サイト (Site)] をクリックします。

ステップ3 [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] 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] 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り、サイト間の既知のユニキャストトラフィックに使用されるすべてのスパインスイッチに導入されます。

ステップ7 [+ TEP プールの追加] 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。

ルーティング可能な TEP プールは、サイト間接続のパブリック IP アドレスに使用されます。

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 ACI マルチサイト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。

ステップ1 Cisco ACI マルチサイト Orchestrator GUI にログインします。

ステップ2 [メインメニュー (Main menu)]で [サイト (Site)] をクリックします。

ステップ3 [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] 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、次の情報を入力します。

- [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。
- [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。[継承 (inherit)] を指定することも、576 ~ 9000 の値を指定することもできます。

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。

- **[OSPF ポリシー (OSPF Policy)]** フィールドで、[インフラの設定: サイトの設定 \(34 ページ\)](#) 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

ステップ 8 **[BGP ピアリング (BGP Peering)]** ノブを有効にします。

2つより多くのスパインスイッチのある単一のポッドファブリックでは、BGP ピアリングは **BGP スピーカ (BGP Speakers)** と呼ばれるスパインスイッチのペア (冗長性のためのもの) 上でのみ有効にします。他のすべてのスパインスイッチでは、BGP ピアリングを無効にします。これらは **BGP フォワーダ (BGP Forwarders)** としてのみ機能します。

マルチポッドファブリック BGP ピアリングは、それぞれが異なるポッドに展開された、2 台の BGP スピーカ スパインスイッチ上でのみ有効にします。他のすべてのスパインスイッチでは、BGP ピアリングを無効にします。これらは BGP フォワーダ (BGP Forwarders) としてのみ機能します。

ステップ 9 **[BGP-EVPN ルータ ID (BGP-EVPN Router-ID)]** フィールドでは、サイト間の BGP-eVPN セッションで使用する IP アドレスを指定します。

ステップ 10 すべてのスパインスイッチで手順を繰り返します。

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 Cisco ACI マルチサイト Orchestrator GUI にログインします。

ステップ 2 [メインメニュー (Main menu)] で [サイト (Site)] をクリックします。

ステップ 3 [サイト (Sites)] ビューで、[インフラ設定 (Configure Infra)] をクリックします。

ステップ 4 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。

インフラストラクチャ設定を各サイトに展開する前に、この章の前の項で説明したように、必要なすべての一般的な設定とサイトローカルの設定が完了していることを確認します。

マルチサイト Orchestrator GUI を使用したサイトの削除

このセクションでは、マルチサイト GUI を使用してサイトを削除する方法を説明します。

- ステップ1 マルチサイト GUI にログインします。
- ステップ2 サイトの削除を試みる前に、どのスキーマからもサイトがアンバインドされていることを確認します。
- ステップ3 **Main menu** で **Sites** をクリックします。
- ステップ4 **Sites List** ページで、さくをするサイトにマウスを合わせて **Action > Delete** を選択します。
- ステップ5 **YES** をクリックします。

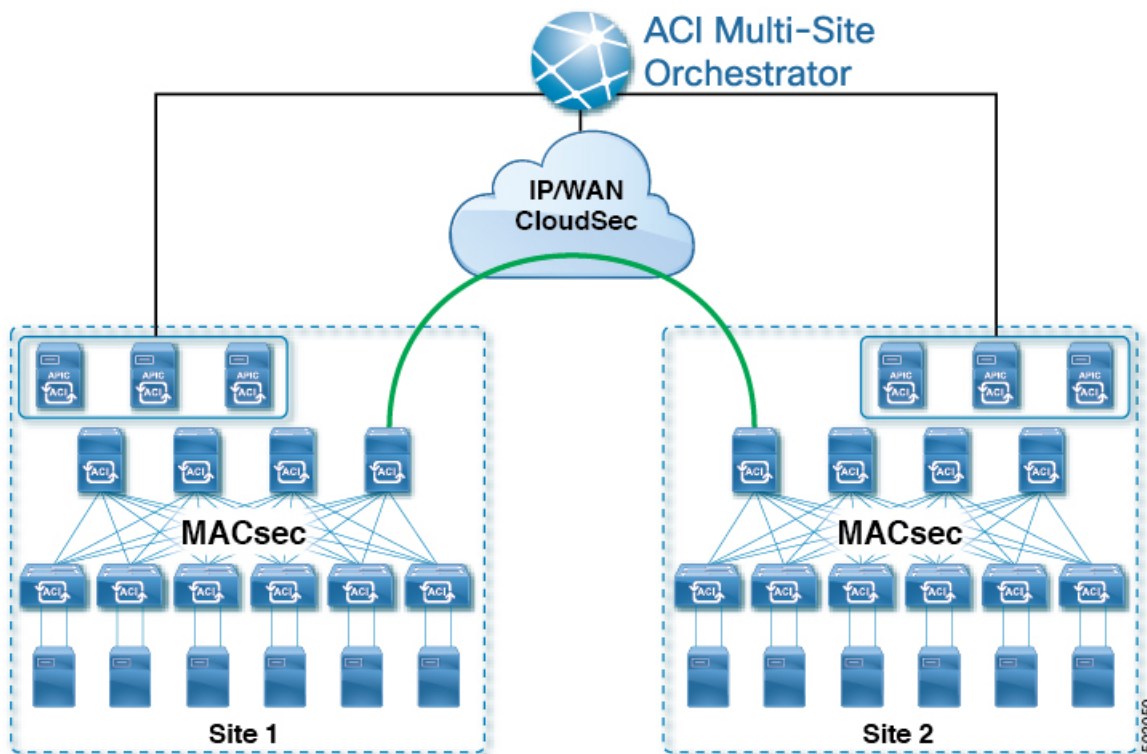
Cisco ACI CloudSec 暗号化

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 Cisco ACI マルチサイト 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、個別のファブリックを相互接続する安全でない外部 IP ネットワークによって接続された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。Cisco ACI マルチサイト 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。

Cisco ACI マルチサイト トポロジはサイト間の接続を提供するために、3 個のトンネルエンドポイント (TEP) IP アドレスを使用します。これらの TEP アドレスは、Cisco ACI マルチサイト 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ます。次いで、それらは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、サイト間トラフィックの暗号化のために、ローカルサイトトラフィックの MACsec と CloudSec を組み合わせる全体的な暗号化アプローチを示しています。

図 11: CloudSec 暗号化



CloudSec の要件とガイドライン

CloudSec 暗号化機能は、リモートリーフダイレクト、仮想ポッド (vPOD)、SDA、サイト間 L3Out、またはその他のルート可能な TEP 設定ではサポートされていません。

ハードウェア要件

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。

ソフトウェアとライセンスの要件

Cisco ACI CloudSec 暗号化には、次のものがが必要です。

- Cisco ACI 各サイトの APIC クラスタを使用したスパイン リーフ アーキテクチャ
- Cisco ACI 各サイトを管理するためのマルチサイト Orchestrator
- ファブリック内のリーフごとの Cisco Digital Network Architecture (DNA) アドバンテージ ライセンス
- 暗号化のためのスパイン スイッチごとのアドオン ライセンス ACI-SEC-GX:
 - 固定スパイン スイッチの場合: ACI-SEC-XF
 - モジュール型スパイン スイッチの場合: ACI-SEC-XM

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応じて、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、リモートサイトによって生成された暗号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化するデータセンター ファブリック。
- TX キー: 平文の 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キー。ACI では、すべてのリモート サイトに対して TX キーを1つだけアクティブにすることができます。
- RX キー: 暗号化された VXLAN パケット ペイロードを復号化するために使用される暗号キー。ACI では、リモートサイトごとに2つの RX キーをアクティブにすることができます。

キーの再生成プロセス中には、2つの RX キーを同時にアクティブにすることができます。ダウンストリーム サイトは、新しいキーの展開が終了した後も、一定時間古い RX キーと

新しい RX キーを保持します。これは、順序どおりでないパケット配信が行われた場合でも、どちらかのキーを使用して適切に復号することができるようにするためです。

- 対称キー：同じ暗号キーを使用して、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) を行います。
- キー再生成: 古いキーの有効期限が切れた後に、アップストリーム サイトが開始する、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プロセスです。
- セキュアチャネル識別子 (SCI): サイト間のセキュリティ アソシエーションを表す、64 ビットの識別子です。CloudSec ヘッダの暗号化パケットで送信され、パケット復号化のためにダウンストリーム デバイスで RX キーを導出するために使用されます。
- アソシエーション番号 (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) です。復号化のため、ダウンストリーム デバイスでキーを取得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できます。キー再生成操作後に、同じアップストリーム デバイスからパケットが順番通りではなく到着した場合でも、処理できるようにするためです。

ACI において、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 と 1) だけが使用されます。任意の時点で、TX キーには、1 つのアソシエーション番号値 (0 または 1) だけが使用されます。

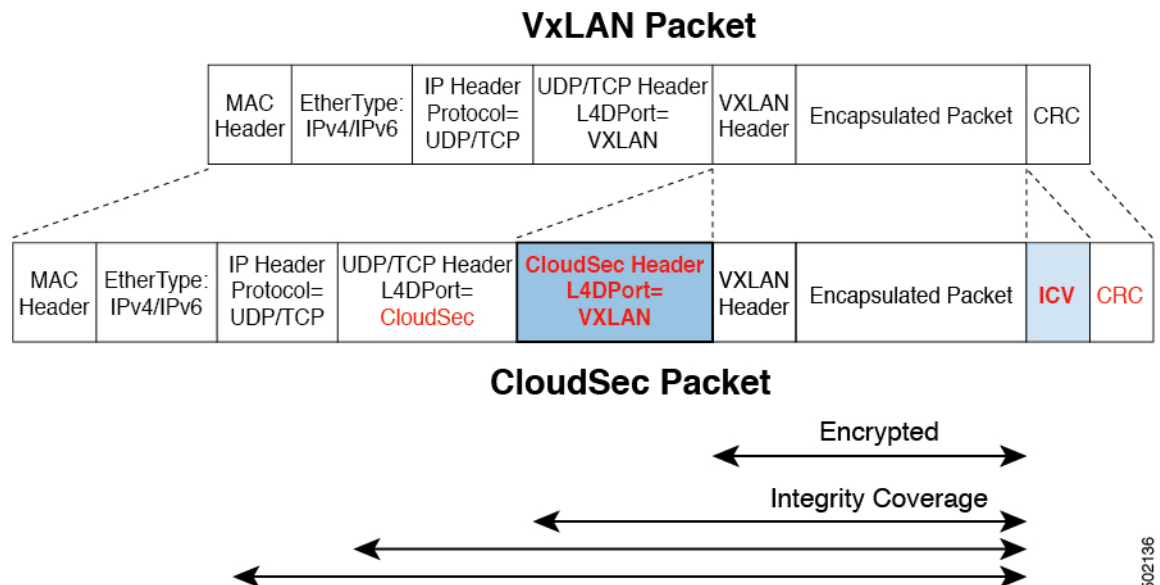
- 事前共有キー (PSK): CloudSec TX および RX キーを生成するためのランダムシードとして使用されるように、Cisco APIC GUI で 1 つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックス順で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64 文字の 16 進数文字列である必要があります。Cisco APIC は最大 256 の事前共有キーをサポートします。

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、Cisco ACI マルチサイトはマルチサイトファブリック間の完全な送信元から宛先への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 12: CloudSec パケット



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 ヘッダーとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、一致する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。
- 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シスコ独自のレイヤ 4 ポート番号 (ポート 9999) で上書きされます。
- [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。

502196

- 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。

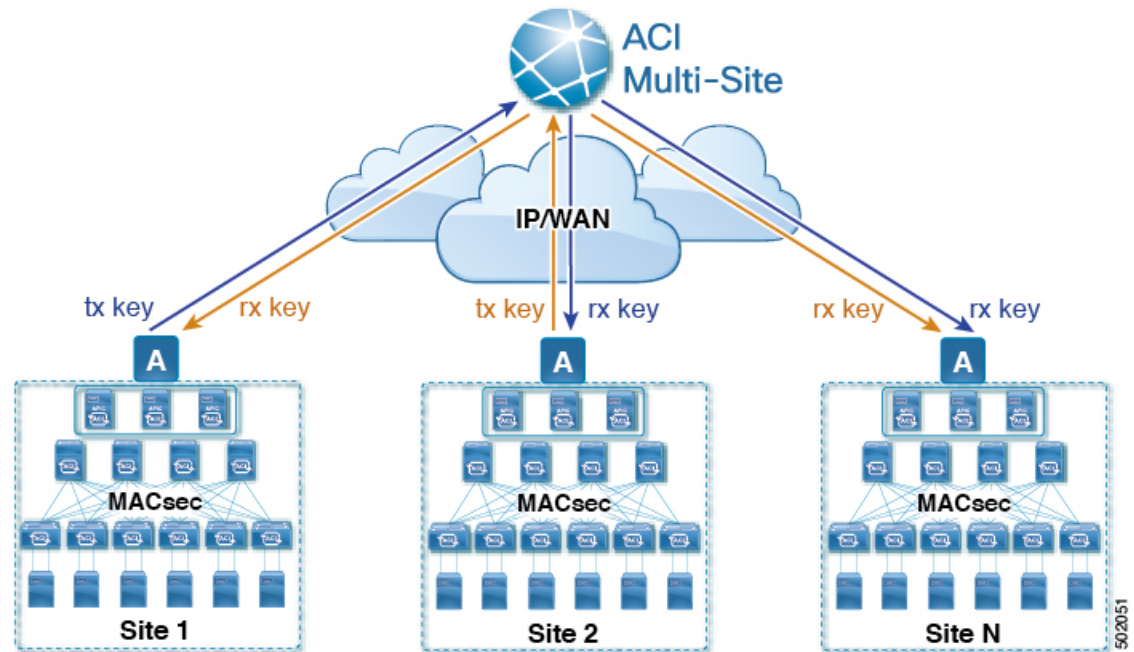
- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

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。
- キーストアが2つ以上の可能な暗号解読キーを返す場合、CloudSec ヘッダーの Association Number (AN) フィールドを使用して、使用するキーを選択します。
- 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 13: 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 Cisco ACI マルチサイト Orchestrator (MSO) にプッシュされます。
- MSO 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。
- 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、MSO にプッシュします。
- MSO 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、MSO 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ります。



(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 \(50 ページ\)](#)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 Cisco ACI マルチサイト Orchestrator への通知に責任をもちます。

Cisco ACI マルチサイト キー管理における Orchestrator の役割

Cisco ACI マルチサイト 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。MSO 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、Cisco ACI 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 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) を設定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。

PSK は暗号キー生成のシードとして使用されるため、複数の PSK を設定すると、生成された暗号キーの過剰な脆弱性が低減され、セキュリティが強化されます。



- (注) Cisco APIC で事前共有キーが設定されていない場合、CloudSec はそのサイトに対して有効にはなりません。その場合、CloudSec 設定を Cisco ACI マルチサイトでオンにすると、エラーが生じます。

新しい PSK で前に追加した PSK を更新したい場合はいつでも、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 \(47 ページ\)](#) の説明に従って、Cisco APIC GUI を使用する
- [NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定 \(48 ページ\)](#) の説明に従って、Cisco APIC NX-OS Style CLI を使用する
- [REST API を使用した CloudSec 暗号化の Cisco APIC の設定 \(49 ページ\)](#) の説明に従って、Cisco APIC REST API を使用する

GUI を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションでは、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 (Tenants)] > [インフラ (Infra)] > [ポリシー (Policies)] > [CloudSec 暗号化 (CloudSec Encryption)] に移動します。

ステップ 3 [SA キーの有効期限 (Sa Key Expiry Time)] 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、キー再設定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 (Pre-Shared Keys)] 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 (Index)] を指定し、その後、[事前共有 (Pre-Shared Key)] キー自体を指定します。

[インデックス (Index)] フィールドでは、事前共有キーを使用する順序を指定します。最後 (最大のインデックス) のキーが使用された後は、プロセスは最初 (最小のインデックス) のキーで続行されます。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(Pre-Shared Key)]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 スタイル 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グレーション モードを入力します。

例：

```
apic1(config)# template cloudsec default
apic1(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、キー再設定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。期限は5～1440分の範囲で入力できます。

例：

```
apic1(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：

```
apic1(config-cloudsec)# pskindex <psk-index>
apic1(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、キー再設定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>
```

Cisco ACI マルチサイト Orchestrator GUI を使用した CloudSec 暗号化の有効化

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す。

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 ACI マルチサイト Orchestrator インストレーションおよびアップグレードガイド』の説明に従って、インストールおよび設定されたCisco ACI マルチサイト Orchestrator。
- 『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Cisco ACI マルチサイト Orchestrator に追加しました。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のサイドバーから、[**サイト (Sites)**] ビューを選択します。

ステップ 3 メインウィンドウの右上にある [**Infra の構成**] ボタンをクリックします。

ステップ 4 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 5 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。

- **通常のデコミッション:** 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。デコミッション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 スタイル CLI を使用したキー再生成プロセスの無効化と再有効化 \(51 ページ\)](#) 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からのデコミッションと削除:** CloudSec キー再生成プロセスは、[NX OS スタイル CLI を使用したキー再生成プロセスの無効化と再有効化 \(51 ページ\)](#) 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 スタイル CLI 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は、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。ここでは、NX OS スタイル CLI を Cisco APIC 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 Cisco APIC NX OS スタイル 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 キー再生成プロセスを停止または再起動します。

キー再生成プロセスを停止するには、次の手順を実行します。

例：

```
apicl(config-cloudsec)# stoprekey yes
```

キー再生成プロセスを再起動するには、次の手順を実行します。

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は、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。ここでは、Cisco APIC REST 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>
```

Cisco APIC への マルチサイトの クロス起動

マルチサイトは現在、テナントを作成してサイトを設定するときに選択する基本パラメータをサポートしています。マルチサイトは、ほとんどのテナント ポリシーをサポートしていますが、いくつかの拡張パラメータを設定することもできます。

マルチサイト GUI を使用して、設定する基本的なプロパティを管理します。高度なプロパティを設定する場合のために、マルチサイト GUI から直接 Cisco APIC GUI をクロス起動する機能が提供されます。Cisco APIC に直接、追加のプロパティを設定することもできます。

APIC にクロス起動できる場所とは別に、3 つの異なるアクセス ポイントが マルチサイト GUI にあります。マルチサイトのこれらのアクセス ポイントから、Cisco APIC へのアクセス権を持つ新しいブラウザ タブを開くことができます。最初に、Cisco APIC にログインします。それから Cisco APIC GUI に関連付けられた画面が表示されます。

サイトから Cisco APIC をクロス起動する

始める前に

- 少なくとも 1 つのサイトは マルチサイト で設定する必要があります。
- サイトでは、少なくとも 1 つ、VRF とブリッジドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

ステップ 1 左側のサイドバーで、[**サイト (Sites)**] ビューを開きます。

ステップ 2 [**サイト (Sites)**] リストから、適切なサイトの名前の上にカーソルを合わせて、行の末尾の [**アクション (Action)**] アイコンをクリックし、[**APIC ユーザ インターフェイスで開く (Open in APIC User Interface)**] を選択して、Cisco APIC GUI にアクセスします。

APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

スキーマからの Cisco APIC のクロス起動

始める前に

- マルチサイトでテンプレートに基づいて少なくとも1つのサイトを設定する必要があります。
- サイトは、少なくとも1つ、VRF とブリッジドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

ステップ 1 左側のサイドバーから、[スキーマ (schema)] ビューを開きます。

ステップ 2 [スキーマ (schema)] リストから、適切な <スキーマ名> をクリックします。

ステップ 3 左側のサイドバーの [サイト (Sites)] リストから、該当するサイトの名前の上にカーソルを移動し、行の最後にある [アクション (Actions)] アイコンをクリックし、[APIC ユーザ インターフェイスで開く (Open in APIC User Interface)] を選択して、Cisco APIC GUI にアクセスします。

APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

プロパティ ペインから Cisco APIC をクロス起動する

始める前に

- 少なくとも1つのサイトはマルチサイトで設定する必要があります。
- サイトは、少なくとも1つ、VRF とブリッジドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

ステップ 1 左側のサイドバーから、[スキーマ (schema)] ビューを開きます。

ステップ 2 [スキーマ (schema)] リストから、適切な <スキーマ名> をクリックします。

ステップ 3 左側のサイドバーの [サイト (Sites)] リストから、適切なサイトを選択します。

ステップ 4 Canvas で、特定のエンティティの名前を選択します。

たとえば、使用可能なVRF、契約、ブリッジドメイン、または必要に応じて別のエンティティを選択します。

その特定のエンティティの詳細が右側の [プロパティ (Property)] ペイン に表示されます。

ステップ 5 [Property] ペインの右上にある [APIC ユーザ インターフェイスで開く (Open in APIC Interface)] アイコンをクリックして、Cisco APIC GUI にアクセスします。

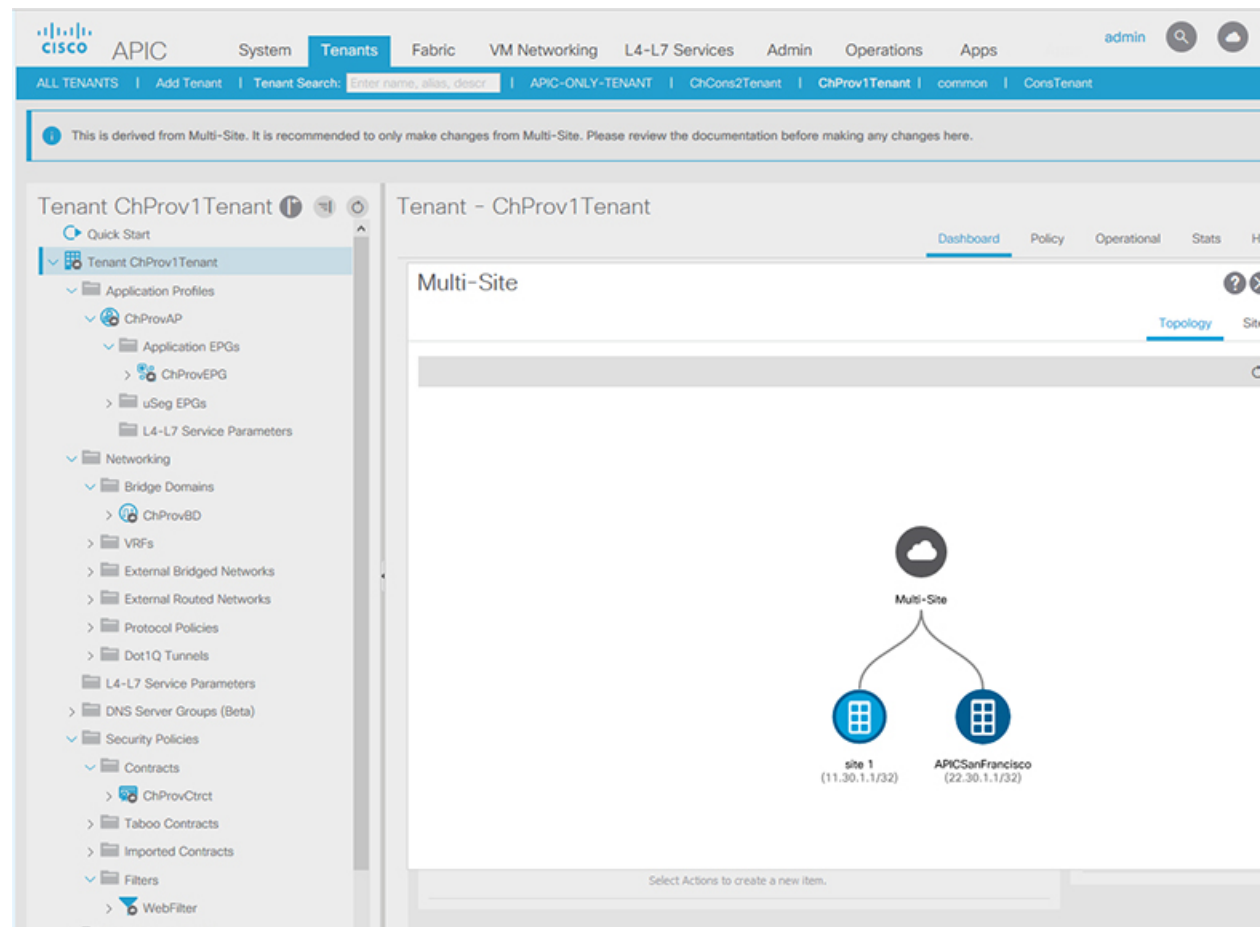
APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

Cisco ACI マルチサイトの管理対象オブジェクトを Cisco APIC GUI を使用して表示する。

Cisco ACI マルチサイトの管理対象オブジェクトを Cisco APIC GUI を使用して表示する。

APIC クラスタが マルチサイト によって管理されている場合、クラウドアイコンが他のサイトとの関係を示します。

図 14: マルチサイトの管理対象オブジェクトを APIC GUI を使用して表示する。



始める前に

APIC クラスタ/サイトは、Cisco ACI マルチサイト を使用して管理されるようセットアップされている必要があります。

ステップ 1 APIC サイトと他のサイトとの関係を表示するには、設定アイコンの隣の、右上にあるクラウドアイコンをクリックします。

図において、ライトブルーのサイトアイコンにマウスを合わせるとローカルサイトの詳細が、ダークブルーのアイコンに合わせるとリモートサイトの詳細が表示されます。

画像において、T1 およびアプリケーションプロファイル、EPG、BD、VRF、および契約には、クラウドのアイコンが付けられます。これは、それらがマルチサイトによって管理されていることを示しています。これらのオブジェクトに変更を加えるには、マルチサイト GUI だけを使用することを推奨します。

ステップ 2 情報ページに **Show Usage** ボタンが表示されている VRF、ブリッジドメイン、またはその他のオブジェクトのローカライズまたは拡大された使用状況を表示するには、次の手順に従います。ここではブリッジドメインと VRF を例にします:

- a) メニューバーで、**Tenants** をクリックして、マルチサイトで管理されているテナントをダブルクリックします。
- b) **Networking > Bridge Domains > BD-name** または **Networking > VRFs > vrf-name** をクリックします。

ステップ 3 **Show Usage** をクリックします。

ここでは、オブジェクトを使用しているノードまたはポリシーを表示できます。

(注) 管理対象のポリシーを変更する場合には、マルチサイト GUI だけを使用することを推奨します。

ステップ 4 この BD または VRF の導入の通知設定を範囲を設定するには、**Change Deployment Settings** をクリックします。**Policy** タブでは、オブジェクトのすべての削除と変更に対する警告を有効にすることができます。

ステップ 5 グローバルな警告を有効または無効にするには、**(Global) Show Deployment Warning on Delete/Modify** チェックボックスをオンまたはオフにします。

ステップ 6 ローカルな警告を有効または無効にするには、**Yes** または **No** を **(Local) Show Deployment Warning on Delete/Modify** フィールドで選択します。

ステップ 7 過去の警告を表示するには、**History** タブ **Events** または **Audit Logs** をクリックします。

■ Cisco ACI マルチサイトの管理対象オブジェクトを Cisco APIC GUI を使用して表示する。



第 4 章

テナント管理

- [テナント管理のガイドライン \(57 ページ\)](#)
- [テナントの追加 \(58 ページ\)](#)
- [テナントまたは Vrf 間でグローバル契約の設定 \(59 ページ\)](#)
- [マルチサイト GUI を使用した EPG 内分離の設定 \(60 ページ\)](#)
- [マルチサイト GUI を使用した マイクロセグメント EPG の設定 \(61 ページ\)](#)
- [Epg を使用して、ドメインに関連付け、マルチサイト GUI \(63 ページ\)](#)
- [統合ビューですべてのテナントを表示する \(64 ページ\)](#)

テナント管理のガイドライン

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。

テナントとそのポリシーは、次の 2 つの方法のいずれかで作成できます。

- APIC サイトから完全に設定済みのテナントをインポートします。
- テナントを作成し、マルチサイト Orchestrator GUI でポリシーを設定します。

次のテナント ポリシーとその関連付けは、マルチサイト Orchestrator GUI で設定できます。

- アプリケーション プロファイルと EPG
- VRF
- サブネットを持ち、拡大またはサイトに合わせてローカライズされた設定を持つブリッジドメイン
- コントラクトとフィルタ
- L3 Out
- 外部 EPG
- EPG との物理または VMM ドメインとの関連付け
- EPG 内分離

- マイクロセグメント化された EPG
- ポート、PC、または VPC に展開された EPG

テナントの追加

このセクションでは、マルチサイト 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 Cisco ACI マルチサイト Orchestrator GUI にログインします。

ステップ 2 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。

ステップ 3 **[表示名 (Display Name)]** フィールドに、テナント名を入力します。

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、Cisco 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。

ステップ 4 (オプション) **[説明 (Description)]** フィールドに、テナントの説明を入力します。

ステップ 5 **[関連付けられたサイト (Associated Sites)]** セクションで、サイトを選択します。

- a) このテナントを使用するテンプレートの展開を予定しているすべてのサイトをオンにします。

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。

(注) MPLS ネットワーク経由で接続されているサイトを選択した場合は、次のようになります。

- b) **[セキュリティ ドメイン (Security Domains)]** フィールドで、ドロップダウン リストからセキュリティ ドメインを選択します。

セキュリティ ドメインは Cisco 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 Cisco APIC のポリシーとユーザアカウントに割り当てることができます。詳細については、*Cisco APIC ベーシック 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 6 **[関連付けられているユーザ (Associated Users)]** セクションで、Orchestrator ユーザを追加します。

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。

ステップ 7 (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 ACI Multi-Site Troubleshooting Guide*を参照してください。

ステップ 8 [保存 (SAVE)] をクリックして、テナントの追加を終了します。

テナントまたは Vrf 間でグローバル契約の設定

この使用例は他のテナントまたは Vrf Epg にサービスを提供するデータセンター用です。サービスを消費するために、すべての Epg の有効化する契約を提供します。

詳細については参照してください、サービス プロバイダー EPG の拡大が共有 使用例で、*Cisco ACI* マルチサイトの基礎ガイド。

始める前に

テナント、Vrf、ブリッジドメイン、アプリケーションプロファイル、Epg、およびその他の契約 (を提供し、サービスを利用するすべてのサイト) のスキーマを作成します。

テナント、Vrf、BDs、および Epg は、サイトをまたぐにする必要はありません。

ステップ 1 プロバイダーのスキーマを開きます。

ステップ 2 次の手順でフィルタ (基本的には、アクセス コントロール リスト) を作成します。

- a) + アイコンをクリックしてフィルタを追加します。
- b) フィルタ名を入力します。
- c) + アイコンをクリックしてエントリを追加します。
- d) エントリ名を入力します。
- e) 残りのフィルタに必要なデータを入力し、をクリックして **保存**。

ステップ 3 次の手順を使用して契約を作成します:

- a) + アイコンをクリックして契約を追加します。
- b) 契約名を入力します。
- c) グローバルには、契約範囲を変更します。
これにより、契約への複数の vrf Epg にアクセスできます。
- d) をクリックします + アイコンをフィルタを追加して、作成したフィルタを選択します。
- e) [Save (保存)] をクリックします。

ステップ 4 次のアクションを契約とサービスを提供する EPG に関連付けます。

- a) EPG をクリックします。
- b) + アイコンをクリックして契約を追加します。
- c) 先補と作成したグローバル契約を選択します。
- d) タイプを設定 **プロバイダー**。
- e) [Save (保存)] をクリックします。

f) をクリックして **サイトを展開**します。サイトを**確認**し、をクリックして **導入**。

ステップ 5 契約を次のアクションを消費者として Epg を関連付けます。

- a) 各コンシューマ スキーマを開きます。
- b) EPG をクリックします。
- c) + アイコンをクリックして契約を追加します。
- d) **契約** フィールドで、契約名の入力を開始します。契約は、リストが表示されたら、それを選択します。
- e) タイプを設定 **コンシューマ**。
- f) **[Save (保存)]** をクリックします。
- g) スキーマの他の Epg に契約を関連付けます。
- h) をクリックして **サイトを展開**します。
- i) サイトを**確認**し、をクリックして **導入**。

マルチサイトGUIを使用した EPG 内分離の設定

内通 EPG 分離が適用される分離が動作している EPG のエンドポイント間で使用できます。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。EPG は、すべての ACI ネットワーク ドメインに分離が適用されているか、またはどのドメインにも適用されていないかのいずれかです。ACI ファブリックは接続エンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN (PVLAN) タグに従って分離規則を認識します。

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

- 分離を適用した EPG 全体のすべてのレイヤ 2 エンドポイント通信がブリッジ ドメイン内にドロップされます。
- 分離を適用した EPG 全体のすべてのレイヤ 3 エンドポイント通信が同じサブネット内にドロップされます。
- トラフィックは、EPG に適用される分離なしの分離適用で、EPG から転送すると、優先順位の設定がサポートされていません QoS CoS を保持します。
- マルチサイト、内通 EPG 分離は AV VLAN モードと DVS VXLAN モードではサポートされていません。適用する内通 EPG の分離を設定すると、これらのドメインにブロックされた状態に移動するポートと可能性があります。
- ブリッジ ドメインが「レガシー BD モード」として設定されている場合、内通 EPG 分離がサポートされていません。

始める前に

- Epg に関連付けられているテナントを作成します。

- テナント ポリシーをインポートまたはテナントの VRF、ブリッジ ドメインがある場合内通 EPG 分離以下 Epg を含むアプリケーション ネットワーク プロファイルを含むスキーマを設定します。

-
- ステップ 1 分離する Epg が設定されているスキーマとテンプレートを開きます。
 - ステップ 2 EPG をクリックします。
 - ステップ 3 **Enforced** を選択し、警告を読み、**OK**を選択します。
 - ステップ 4 オプション。その他の Epg に分離適用を設定します。
 - ステップ 5 サイトの場所に配置されます (内通 EPG 分離に設定されている) Epg を含むテンプレートにプッシュします。
 - ステップ 6 導入のサイトとテンプレートをクリックし、**EPG]** をクリックします。
 - ステップ 7 **ADD STATIC PORT** をクリックします。
 - ステップ 8 選択、 **パスのタイプ** (ポート、ポート チャンネルを直接、またはバーチャル ポート チャンネル)。
 - ステップ 9 **LEAF** を選択します。
 - ステップ 10 **PATH** を選択します。
 - ステップ 11 **ポート ENCAP VLAN** フィールドで、EPG のトラフィックに使用する VLAN 番号を入力します。
 - ステップ 12 **導入即時** フィールドで、選択 **オンデマンド** または **即時** 導入します。
 - ステップ 13 **モード** フィールドで、選択 **トランク** 。
 - ステップ 14 オプションで、他の適用の分離を持つ Epg の手順を繰り返します。
-

次のタスク

変更を Epg が配置されているサイトにプッシュします。

マルチサイト GUI を使用した マイクロセグメント EPG の設定

Cisco ACI マルチサイト を使用してマイクロセグメンテーションを設定し、ネットワークベースの属性 (IP、MAC、DNS) または VM ベースの属性 (VM ID、VM 名、VMM ドメインなど) を使用する、属性ベースの EPG を作成することができます。これにより、1 つの基本 EPG 内の VM または物理エンドポイント、または異なる EPG の VM または物理エンドポイントを分離することができます。

Cisco ACI マルチサイトで設定できるのは、マイクロセグメント (uSeg) EPG の基本的なオプションだけです。高度なオプションと使用例、およびマイクロセグメント化された EPG の詳細については、「*Microsegmentation with Cisco ACI*」の章『*Cisco ACI Virtualization Guide, Release 3.0*』参照してください。



(注) EPG を作成するとき、まずアプリケーション EPG を作成し、後ほどそれを uSeg EPG に変更する場合には、EPG に別の名前を割り当てるか、次の手順で、アプリケーション EPG を削除してから uSeg EPG を追加する必要があります:

1. スキーマからアプリケーション EPG を削除します。
2. サイトにスキーマを展開します。
3. uSeg EPG を作成します。
4. サイトにスキーマを再配置します。

Cisco ACI マルチサイト を使用してマイクロセグメント化された EPG を設定するには、次の手順に従います:

始める前に

- マイクロセグメント化される EPG に関連付けられるテナントを作成します。
- テナントポリシーをインポートするか、またはテナントの VRF、ブリッジドメイン、EPG を含むアプリケーション ネットワーク プロファイルを含むスキーマを設定します。
- テナントでは少なくとも 1 つのアプリケーション EPG を作成します。

ステップ 1 EPG が設定されているスキーマを開きます。

ステップ 2 EPG をクリックします。

ステップ 3 **USEG EPG.** をクリックします。

ステップ 4 **ADD USEG ATTRIBUTES** をクリックします。

ステップ 5 [DISPLAY NAME] フィールドで、属性の名前を入力します。

ステップ 6 **ATTRIBUTE TYPE** を選択します。これは次のいずれかになります:

- **IP**
- **Mac**
- **[DNS]**
- **VM Name**
- **VM Data Center**
- **VM Hypervisor Identifier**
- **VM Operating System**
- **VM Tag**
- **VM Identifier**

- VM VMM Domain
- VM VNIC DN (vNIC ドメイン名)

ステップ7 変更を保存します。

次のタスク

マルチサイト GUI を使用して、uSeg EPGをドメインに関連付けます。

Epgを使用して、ドメインに関連付け、マルチサイトGUI

始める前に

- [Epg に関連付けられているテナントを作成 Cisco ACI マルチサイト します。
- ドメインプロファイル(VMM、L2、L3、またはファイバチャネル)を作成 APIC します。
- テナントのポリシーをインポート Cisco APIC(テンプレート)を持つスキーマを設定またはマルチサイト、テナントの VRF、ブリッジドメインおよびドメインに関連付けられる Epg を含むアプリケーション ネットワーク プロファイルが含まれています。
テンプレートをサイトと関連付けます。

ステップ1 サイト リストをサイトと場所 EPG とドメインが設定されて、サイトのテンプレートをクリックして、EPG をクリックします。

ステップ2 **ADD DOMAINS** をクリックします。

ステップ3 **ドメイン アソシエーション タイプ** フィールドで、できるタイプを選択します。

- VMM
- Fibre Channel
- L2 外部
- L3 外部
- 物理

ステップ4 **ドメイン プロファイル** フィールドで、以前に作成したプロファイルを選択または **物理サイズ** 。

ステップ5 **導入即時** フィールドで、選択 **オンデマンド** または **即時** 。

ステップ6 **解像度即時** フィールドで、選択 **オンデマンド** 、 **即時** 、または **事前プロビジョニング** 。

ステップ7 変更を保存します。

次のタスク

サイトへの変更を含むテンプレートにプッシュします。

統合ビューですべてのテナントを表示する

マルチサイト GUI の **Tenants** タブを使えば、テナントの集約リストを表示できます。

Tenants パネル (**Tenants** タブの下) には、次のフィールドが GUI 内で表示されます:

- **NAME**: テナントの名前です。
- **DESCRIPTION**: テナントごとの説明です。
- **ASSIGNED TO SITES**: テナントが割り当てられているサイトの数です。
- **ASSIGNED TO USERS**: テナントが割り当てられているユーザーの数です。
- **ASSIGNED TO SCHEMAS**: テナントが割り当てられているスキーマの数です。
- **ACTIONS**: テナントごとに実行できるアクションです。 **Edit (編集)**、 **Delete (削除)**、またはそのテナントの **Network Mappings (ネットワーク マッピング)** の構成があります。

Tenants チャートに基づいてテナントのリソース使用率を決定することができます。



第 5 章

ユーザ管理

- ユーザ、ロール、および権限 (65 ページ)
- ユーザ管理上のガイドライン (67 ページ)
- ユーザの追加 (67 ページ)
- ユーザの管理 (68 ページ)

ユーザ、ロール、および権限

Cisco ACI マルチサイト Orchestrator では、ロールベース アクセス コントロール (RBAC) を介して定義されたユーザのロールに従ってアクセスが提供されます。ロールは、ローカルと外部認証の両方に使用されます。Cisco ACI マルチサイト Orchestrator では、次のユーザ ロールを使用できます。

- パワー ユーザー—ユーザがすべての操作を実行できるロール。
- サイト マネージャ—ユーザがサイト、テナント、およびそれらの間の関連付けを管理できるようにするロール。
- スキーマ マネージャ—スキーマ マネージャは、テナントの関連付けに関係なくすべてのスキーマを管理できます。
- スキーマ エディタ: ユーザが明示的に関連付けられているテナントを1つ以上含むスキーマを管理するためのロール。
- ユーザおよびロール マネージャ — ユーザおよびロール マネージャは、すべてのユーザ、そのロール、およびパスワードを管理できます。

上記の各ロールは一連の権限に関連付けられており、これを使用して、Orchestrator GUI のユーザのビューから関連性のない要素を表示し、無関係な要素を非表示にします。たとえば、ユーザ マネージャ ロールにはユーザ関連の権限のみが関連付けられているため、そのロールを持つユーザは GUI の **[ユーザ(User)]** および **[管理 (Admin)]** タブのみを表示できます。

ユーザ ロールおよび権限

次の表は、利用可能なユーザロールごとに許可された Cisco ACI マルチサイトの権限の一覧表示です。属性値 (AV) 列は、Multi-Site Orchestrator で使用する外部認証サーバを設定するときに必要なユーザ設定文字列を指定します。外部認証の詳細については、「管理操作」の章を参照してください。

表 2: ユーザロール

ユーザ ロール	権限	属性値 (AV) のペア
パワー ユーザ	<ul style="list-style-type: none"> ダッシュボード サイト スキーマ テナント ユーザ トラブルシューティングレポート 	shell:misc-roles=powerUser
サイト マネージャ	<ul style="list-style-type: none"> ダッシュボード—サイト サイト テナント 	shell:misc-roles=siteManager
スキーマ マネージャ	<ul style="list-style-type: none"> ダッシュボード—サイトとスキーマの健全性 スキーマ 	shell:misc-roles=schemaManager
スキーマ エディタ	<ul style="list-style-type: none"> ダッシュボード—サイトとスキーマの健全性 スキーマ 	shell:misc-roles=schemaEditor
ユーザ マネージャ	<ul style="list-style-type: none"> ユーザ 	shell:misc-roles=userManager

管理者ユーザ

初期の設定スクリプトで、デフォルト 管理者ユーザアカウントが設定され、システムが起動したときにの唯一のユーザとなります。管理者ユーザの初期パスワードはシステムによって設定され、最初のログイン後に変更するように求められます。

- 管理者ユーザのデフォルトのパスワードは We1come2misc!
- 管理者ユーザは、電力ユーザのロールが割り当てられます。

- 管理者ユーザを使用して、ほかのユーザを作成しその他すべてのDay-0設定を実行します。
- 管理者ユーザのアカウントステータスは、[非アクティブ]に設定できません。

読み取り専用アクセス

上記の各ユーザロールを読み取り専用モードで割り当てることができます。読み取り専用権限が付与されている場合、ユーザは以前と同様に、そのロールで使用可能な任意のファブリックオブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

ユーザ管理上のガイドライン

- ユーザ認証と認可は、ローカルまたは外部を指定できます。外部認証では、RADIUS、TACACS +、またはLDAPサーバを使用できます。外部認証の詳細については、管理操作の章の[外部認証 \(125 ページ\)](#) を参照してください。
- ローカルおよび外部認証の両方で、すべてのユーザ[^]に少なくとも1つのロールを関連付ける必要があります。ユーザは複数のロールに関連付けることができます。複数のロールにユーザに関連付けると、ユーザはオブジェクトの組み合わせにアクセスできるようになります。
- テナントまたはスキーマを使用する前に、ユーザがテナントに関連付けられている必要があります。
- リリース 2.1(2)以降では、ユーザは読み取り専用モードでロールを割り当てることができます。読み取り専用権限が付与されている場合、ユーザは以前と同様に、そのロールで使用可能な任意のファブリックオブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

読み取り専用ユーザロールを設定してから、マルチサイト Orchestrator を以前のバージョンにダウングレードした場合、読み取り専用権限はサポートされません。これらのロールは、すべてのユーザから削除されます。これは、読み取り専用ロールのみを持つすべてのユーザにロールが割り当てられず、削除されることも意味します。パワーユーザまたはユーザマネージャは、ユーザを再度作成し、新しい読み取り/書き込みロールを割り当てる必要があります。

ユーザの追加

このセクションでは、Multi-Site Orchestrator ユーザの作成方法を説明します。

- ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。
- ステップ 2 メインメニューから、[ユーザ (Users)] を選択します。
- ステップ 3 メインウィンドウペインの右上隅で、[ユーザの追加 (Add User)] をクリックします。
- ステップ 4 [Add User (ユーザの追加)] ページで、次を指定します。

- a) [ユーザ名] フィールドに、ユーザ名を入力します。
- b) [パスワード (Password)] および[パスワードの確認 (Confirm Password)] フィールドにユーザのパスワードを入力します。

パスワードは、以下のルールに従う必要があります。

- 長さが少なくとも 12 文字を含む
- 少なくとも 1 個の英字を含む
- 少なくとも 1 つの数字を含むこと
- *およびスペースとは異なる、少なくとも 1 つの特殊文字を含む

- c) [名 (First Name)] フィールドに、ユーザの名を入力します。
- d) [姓 (Last Name)] フィールドに、ユーザの姓を入力します。
- e) [電子メール] フィールドに、ユーザの電子メールアドレスを入力します。
- f) [電話番号] フィールドに、ユーザの電話番号を入力します。
- g) [アカウント ステータス] フィールドで、アカウント ステータスを選択します。

ユーザをアクティブ (Active) または非アクティブ (Inactive) ステータスに設定します。アクティブなユーザのみがマルチサイト Orchestrator にログインできます。

ステップ 5 ユーザ ロール リストで、追加する新しいユーザには、1 つ以上のユーザ ロールを割り当てます。

すべてのユーザに少なくとも 1 つのロールを関連付ける必要があります。ユーザは複数のロールに関連付けることができます。複数のロールにユーザに関連付けると、ユーザがアクセスできる機能の組み合わせが用意されます。

使用可能な各ロールは、読み取り専用モードで設定できます。読み取り専用ロールが付与されている場合、ユーザはそのロールで使用可能な任意のファブリック オブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

ステップ 6 [保存 (Save)] をクリックします。

ユーザの管理

このセクションでは、既存のユーザを編集または削除する方法について説明します。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 自分のパスワードを更新する場合は...

- a) 画面の右上にある [ユーザ (User)] のアイコンをクリックします。
- b) [パスワードのリセット (Reset Passwords)] を選択します。

ステップ 3 ユーザを削除する場合は...

- a) メインメニューから、[ユーザ (Users)] を選択します。

- b) ユーザ名の横にある [アクション(action)] アイコンをクリックして、**[削除 (Delete)]** を選択します。
デフォルトの admin ユーザは削除できません。

ステップ 4 既存のユーザとその権限を編集する場合には...

- a) メインメニューから、**[ユーザ (Users)]** を選択します。
 - b) ユーザ名の横にある [アクション(action)] アイコンをクリックして、**[編集 (Edit)]** を選択します。
デフォルトの admin ユーザの名前、アカウントのステータス、およびロールは変更できません。
admin ユーザ、または **[パワー ユーザ (Power User)]** または **[ユーザ マネージャ (User Manager)]** ロールに関連付けられているユーザは、他のユーザのパスワードを更新できます。最初のログイン時には、ユーザは自分のパスワードを更新するように求められます。
-



第 6 章

スキーマ管理

- スキーマ設計上の考慮事項 (71 ページ)
- スキーマテンプレートの作成 (76 ページ)
- テンプレート間でのオブジェクトの移行 (82 ページ)
- シャドウ EPG と BD (84 ページ)
- サイト内 L3Out (85 ページ)
- EPG 優先グループ (96 ページ)
- レイヤ 3 マルチキャスト (98 ページ)

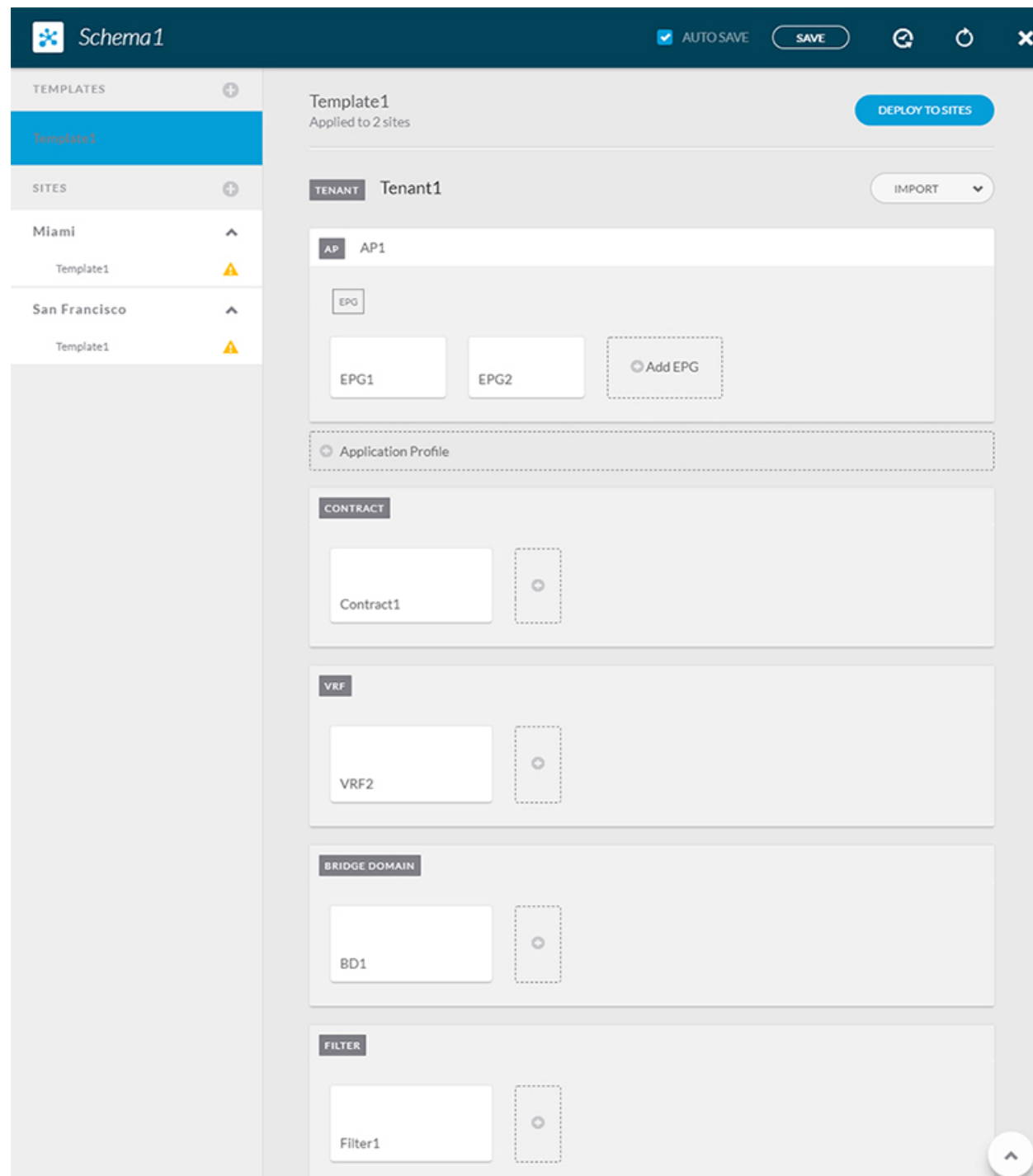
スキーマ設計上の考慮事項

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際には、スキーマの数、テンプレートの数、およびスキーマあたりのオブジェクト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、お使いのリリースに固有の [CISCO APIC](#)、[CISCO ACI Multi-Site](#)、および [Cisco Nexus 9000 シリーズ ACI モードのスイッチの検証済みスケーラビリティガイド](#) を参照してください。

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、単一のテンプレートを展開することです。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することができます。その後、1つのアプリケーションプロファイルまたは複数のアプリケーションプロファイルをテンプレート内に作成し、それを1つ以上のサイトに展開することができます。

図 15: 単一スキーマ



マルチサイトスキーマ作成に対するこの簡単なアプローチを上図に示します。この場合、すべてのオブジェクトが同じスキーマ内で簡単に表示できるようになります。ただし、スキーマごとにサポートされているスキーマまたはテンプレートの数に制限があるため、このアプローチは、これらの制限を超える可能性があるような、大規模な展開には適していません。

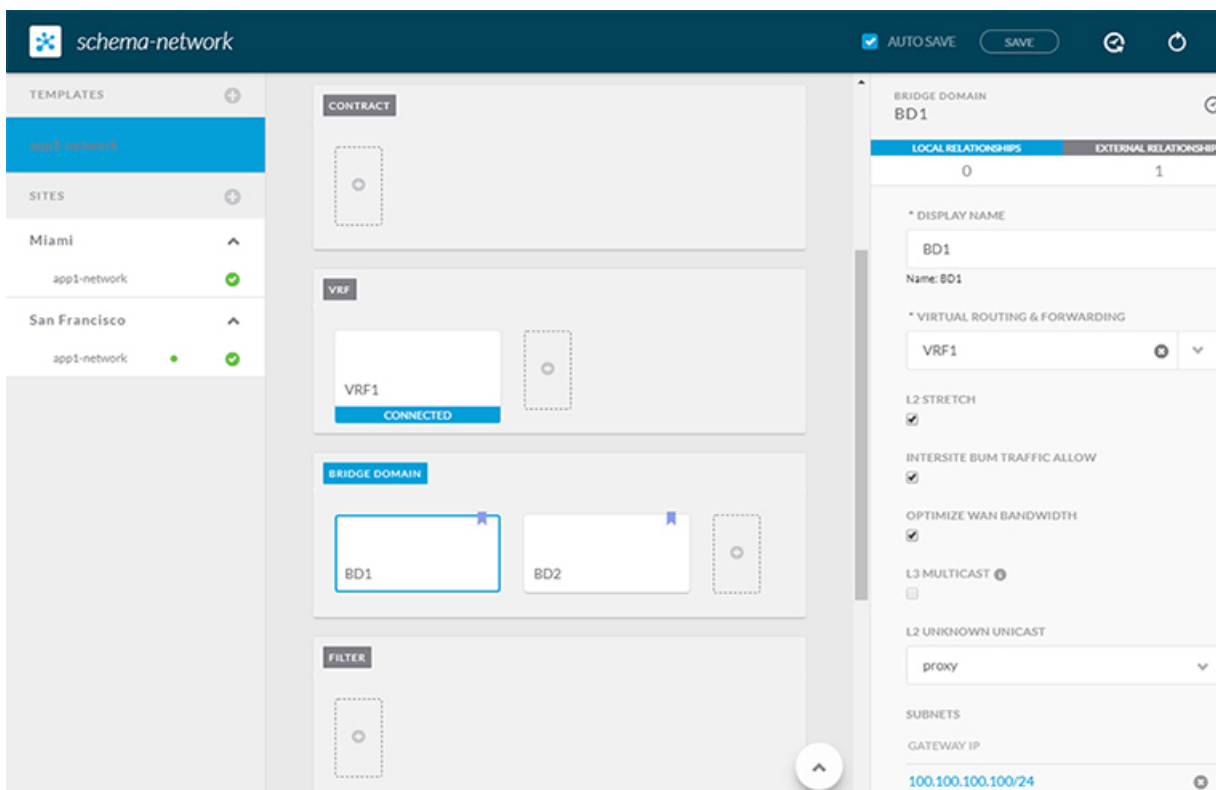
ネットワーク分離での複数スキーマ

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。

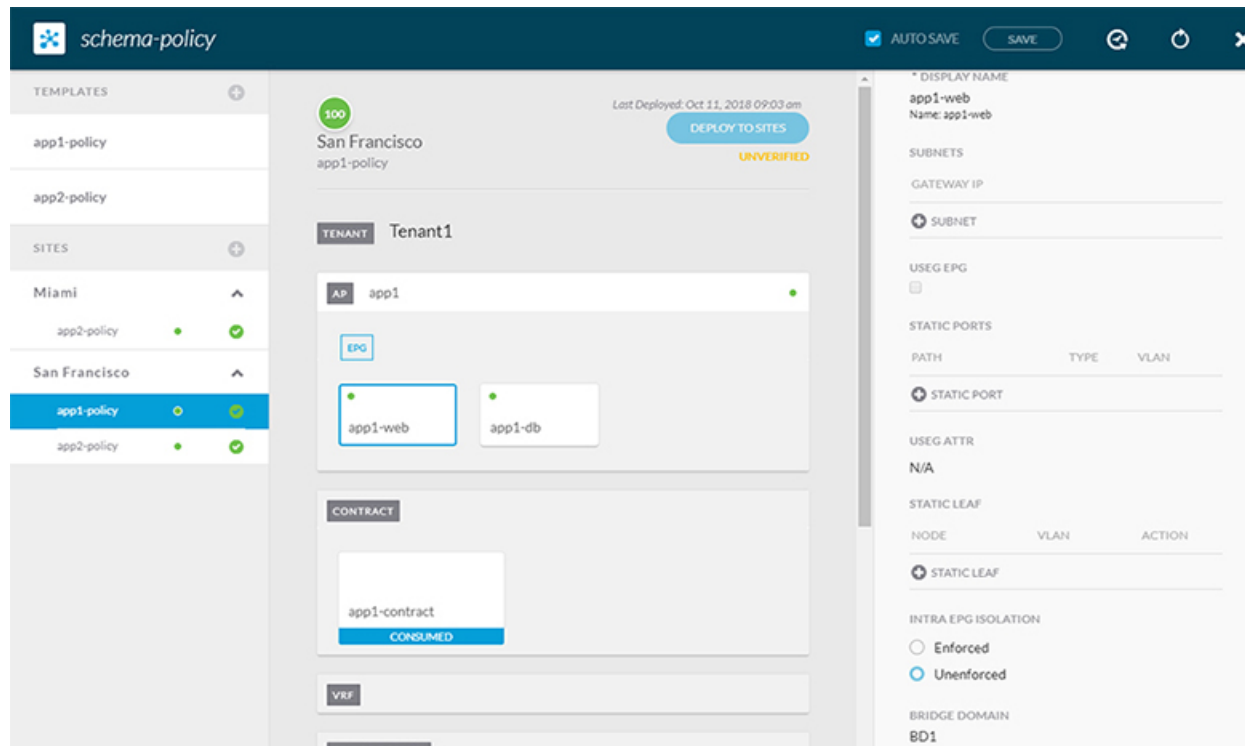
次の図は、VRF、BD、およびサブネットが設定され、2 つのサイトに展開されている単一のネットワークング テンプレート設定を示しています。

図 16: 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ング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 17: ポリシースキーマ



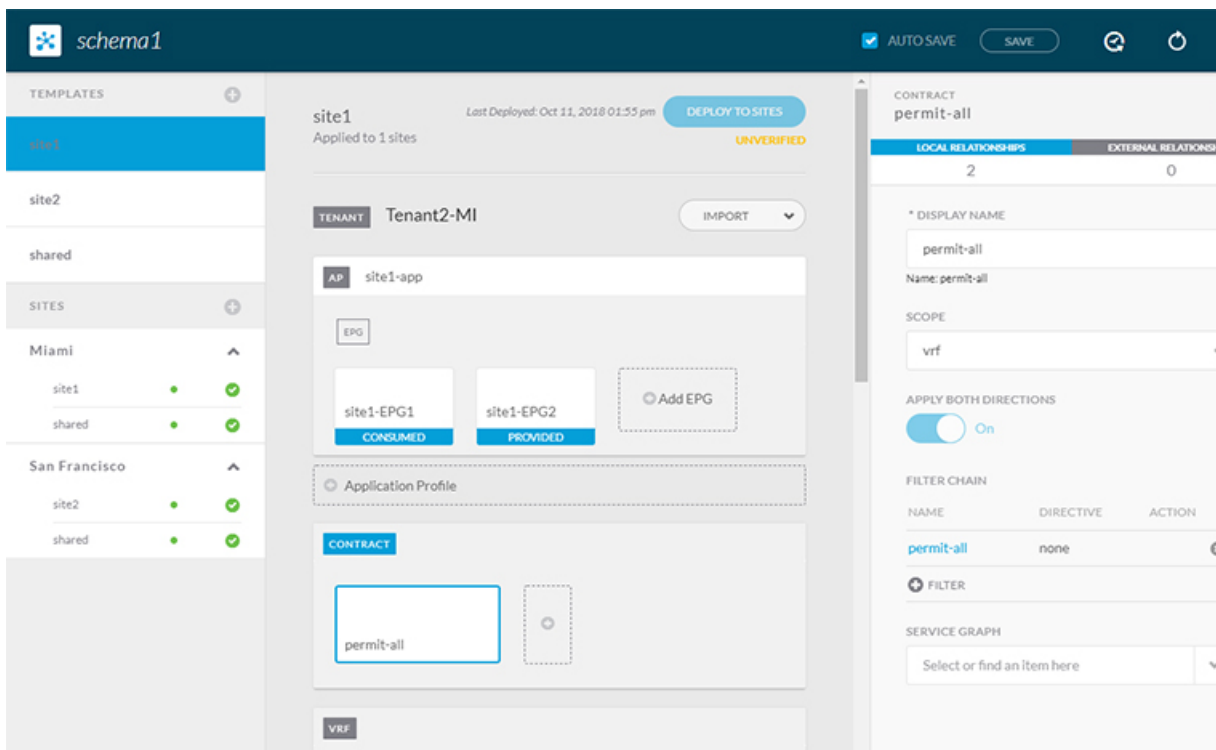
ポリシースキーマとテンプレートを作成して展開すると、ネットワークスキーマのネットワークオブジェクトに、ポリシースキーマ要素による外部参照の数が表示されます。外部参照を含むオブジェクトは、上のネットワークスキーマの図に示すように、リボンのアイコンでも示されます。

この方法で設計されたスキーマは、ネットワーク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 18: 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に5つのテンプレートという制限を超えるため、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。

使用例のCisco Cloud APICスキーマ設計

Cisco ACI マルチサイトは、リリース 2.1(1) 以降の Amazon Web SERVICES (AWS) とリリース 2.2(1) 以降の Microsoft Azure にインストールされたインストールされた Cisco Cloud APIC をサポートしています。Each cloud deployment can be added to and managed by the マルチサイト Orchestrator as its own APIC site.

次のセクションでは、スキーマの作成と管理に必要な一般的な手順について概説していますが、クラウド APIC サイトでサポートされる特定の使用例のシナリオについては、次のクラウド APIC ドキュメントのランディングページ <https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html> にある設定例で詳しく説明されています。

スキーマ 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。
- Cisco APIC テナント ユーザ 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 \(58 ページ\)](#) を参照してください。

ステップ 1 [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。

ステップ 2 [名称未設定のスキーマ (Untitled Schema)] ページで、作成するスキーマの名前を入力します。

ステップ 3 [テナントの選択 (Select A Tenant)] ダイアログ ボックスにアクセスし、ドロップダウン メニューからテナントを選択します。

- (注) 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 \(58 ページ\)](#) を参照してください。

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。

- 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ます。
- ステップ 4** オブジェクトをインポートするサイトを選択します。
- ステップ 5** [インポート (Import)] 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) マルチサイト Orchestrator 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。

アプリケーション プロファイルの設定

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。

- ステップ 1** スキーマ編集ビューで、[+ アプリケーション プロファイル (+ Application Profile)] をクリックします。
- ステップ 2** 右側の [プロパティ (properties)] ペインで、アプリケーション プロファイル名を入力します。
- ステップ 3** [AP <名前>] エリアで、[+ EPG の追加 (+ Add EPG)] をクリックして EPG を追加します。
- ステップ 4** 右側の [プロパティ (properties)] ペインで、EPG の名前を入力します。
- ステップ 5** EPG のコントラクトを追加します。
- [+ コントラクト (+ Contract)] をクリックします。
 - [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。
 - [保存 (SAVE)] をクリックします。
- ステップ 6** [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 7 (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。

- [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。
- [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。
- 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。
- 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。
- [OK]** をクリックします。

ステップ 8 (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。

- [uSeg EPG]** チェックボックスをオンにします。
- [+uSeg EPG]** をクリックします。
- uSeg 属性の **[名前 (Name)]** と **[タイプ (Type)]** を入力します。
- 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。

- [保存 (SAVE)]** をクリックします。

ステップ 9 (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。

ステップ 10 (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 \(98 ページ\)](#)

ステップ 11 (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 \(96 ページ\)](#)

テナントの VRF を設定する

このセクションでは、VRF の設定方法を説明します。

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、[VRF] エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、VRF の名前を入力します。

ステップ 3 (オプション) VRF 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 \(98 ページ\)](#)

ブリッジ ドメインの設定

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、[ブリッジ ドメイン (Bridge Domain)] エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側のプロパティ ペインで、以下のブリッジ ドメインの詳細を入力します。

- [表示名 (Display Name)] フィールドに BD 名。
- [仮想ルーティングと転送 (Virtual Routing and Forwarding)] フィールドに VRF。
- 必要に応じて、[L2 ストレッチ (L2 STRETCH)] チェックボックスをオンにします。
- [L2 ストレッチ (L2 STRETCH)] を有効にした場合は、[サイト間 BUM トラフィックを許可 (INTERSITE BUM TRAFFIC ALLOW)] も有効にできます。
- [L2 ストレッチ (L2 STRETCH)] を有効にしていない場合は、[L2 不明なユニキャスト (L2 UNKNOWN UNICAST)] フィールドの [プロキシ (proxy)] または [フラッド (flood)] を選択できます。

ステップ 3 (オプション) ブリッジ ドメインに 1 つまたは複数のサブネットの追加を選択できます。

- a) [+サブネット (+Subnet)] をクリックします。
[サブネットの追加 (Add 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を入力します。
- c) [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)] を選択します。
- d) 必要に応じて、[VRF 間で共有 (Shared Between VRFs)] をオンにします。
- e) 必要に応じて、[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] をオンにします。
- f) 必要に応じて、[クエリア (Querier)] チェックボックスをオンにします。
- g) [保存 (SAVE)] をクリックします。

コントラクトのフィルタの設定

ここでは、コントラクトのフィルタを設定す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 [スキーマ編集 (Schema edit)] ビューで、[フィルタ (Filter)] エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、フィルタの名前を入力します。

ステップ 3 [+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。

開いた [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。

- a) フィルタ エントリの名前。
- b) (オプション) フィルタ エントリの説明。
- c) EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

- **EtherType**—IP
- **[IP プロトコル (IP Protocol)]**—tcp
- **宛先ポートの範囲 (先頭) (Destination Port Range From):** https
- **宛先ポートの範囲 (末尾) (Destination Port Range To):** https

- d) [保存 (SAVE)] をクリックします。

コントラクトの設定

このセクションでは、コントラクトの設定方法を説明します。

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、[コントラクト] エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側のプロパティ ペインで、コントラクトの名前を入力します。

ステップ 3 ドロップダウン メニューを使用して、[範囲 (Scope)] の値を選択します。

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
- tenant

- global

ステップ 4 [両方向の適用 (Apply Both Direction)] トグル ボタンをクリックして、コントラクトで指定されたフィルタを一方向または両方向に適用します。

デフォルトの設定は [ON] です。

ステップ 5 コントラクト フィルタを追加します。

- a) [+フィルタ (+ Filter)] をクリックします。
- b) [フィルタ チェーンの追加 (Add Filter Chain)] ダイアログで、[名前 (Name)] フィールドをクリックして、フィルタを選択するか検索します。
- c) (オプション) [指令 (Directives)] フィールドで、使用可能な指令を選択します。
- d) [保存] をクリックします。

ステップ 6 [両方向に適用 (Apply Both Direction)] オプションを無効にした場合は、もう一方の方向に2番目のフィルタチェーンを追加します。

外部 EPG の設定

このセクションでは、外部 EPG を設定する方法について説明します。

始める前に

- テナントと VRF が拡大するすべてのサイト上の Cisco APIC 内で L3Out を作成します。
- 各 L3Out の VRF は、すべてのサイトで同じである必要があります。VRF の変更 APIC 外部 Epg を展開した後、L3Out をリセットし、再設定し、サイトの外部 EPG を再配置必要があります。

ステップ 1 [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] します。

ステップ 2 右側の [プロパティ (properties)] ペインで、外部 EPG のタイプを選択し、名前を指定します。

クラウド外部 EPG の詳細については、Cisco Cloud APIC のマニュアルを参照してください。

ステップ 3 [仮想ルーティングと転送 (Virtual Routing & Forwarding)] ドロップダウンから、この外部 EPG に関連付ける VRF を選択します。

ステップ 4 EPG が通信するために必要なコントラクトを追加します。

- (注) 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 [オンプレミスプロパティ (On-Prfem Properties)] エリアで、この外部 EPG の L3Out を選択します。

L3Out の設定

このセクションでは、マルチサイト Orchestrator GUI を使用して L3Out 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 L3Out 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。VRF も Orchestrator で作成されるので、L3Out を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

ステップ1 [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。

ステップ2 右側の [プロパティ (properties)] ペインで、L3Out の表示名と、それに対応する仮想ルーティングおよび転送 (VRF) を入力します。

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。マルチサイト 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。

これらのマルチサイト Orchestrator GUI ページの機能の詳細については、[Cisco ACI マルチサイト Orchestrator GUI の概要 \(3 ページ\)](#) を参照してください。

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異なるテンプレートとスキーマに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する必要があります。
- 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** マルチサイト Orchestrator 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、**[スキーマ (schema)]** を選択します。
- 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。
-

シャドウ EPG と BD

拡張 VRF または共有サービスの使用例において、サイトローカル EPG 間にコントラクトが存在し、プロバイダとコンシューマが異なる VRF にあり、テナント コントラクトを通じて通信する場合、EPG とブリッジドメイン (BD) はリモートサイトでミラーリングされます。これらの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ますが、実際にはサイトの1つだけに展開されています。これらのミラーされたオブジェクトは、「シャドウ EPG または BD」と呼ばれます。

たとえば、プロバイダ サイト グループのテナントと VRF がサイト 1 とサイト 2 に拡張され、コンシューマ サイト グループのテナントと VRF がサイト 3 とサイト 4 に拡張されている場合、サイト 1、サイト 2、サイト 3、サイト 4 の APIC GUI では、両方のテナントとポリシーを表示できます。これらは、それぞれのサイトに直接展開されている場合と同じ名前が表示されます。

シャドウ オブジェクトはまた、優先グループ、vzAny、Layer3 マルチキャスト使用例でも作成されます。



(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。

以下のオブジェクトは、サイト間で拡大するときにシャドウできます。

- 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

APIC GUI でシャドウ オブジェクトを選択する場合、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 よりプッシュされたシャドウ オブジェクトです。このオブジェクトは、変更を加えたり、削除したりしないでください。メイン GUI ペインの上部にの警告が表示されます。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ため、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。これらのオプションについては、次のように確認できます。

ステップ 1 同じ名前を持つ EPG のペアのうちのシャドウ EPG を識別するには、APIC GUI で、[テナント (Tenants)] > [<テナント名>] > [アプリケーション プロファイル (Application Profiles)] > [<アプリケーションプロファイル名>] > [アプリケーション EPG (Application EPGs)] > [<EPG 名>] > [静的ポート (Static Ports)] を選択します。

シャドウ EPG には、静的ポートへのパスはありません。

EPG に VM のみが含まれる VMM ドメイン インテグレーションでは、スタティック ポートもないため、この方法を使用してそれらをシャドウ EPG から区別できないことに注意してください。

ステップ 2 同じ名前を持つ BD のペアのうちのシャドウ BD を識別するには、APIC GUI で、**Tenants > tenant-name > Networking > Bridge Domains > bd-name > Subnets > subnet-name** を選択します。

シャドウ BD のサブネットでは、[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)] が有効になっています。

サイト内 L3Out

リリース 2.2(1) 以前、Multi-Site 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ありました。

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。

L3Out とアプリケーション EPG は、同じまたは異なる VRF とテナントに存在することができます。

- サイト間の L3Out のトランジット—別のサイトの 外部 EPG のエンドポイントと通信する 1 つのサイトの外部 EPG のエンドポイント。

外部 EPG は、同じまたは異なる VRF とテナントに存在することができます。

- サイト間 L3Out の共有サービス—異なる VRF の間での L3Out の共有またはトランジット。

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。
- 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、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。

L3Out がスキーマ テンプレートで定義されている場合、既存の外部 EPG に対して使用できません。

- 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。

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 に保存されません。

- 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 MSO 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、両方が同じテナントにある必要があります。
- 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 マルチサイトのサイト間 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

ルーティング可能な TEP アドレスの設定

サイト間 L3Out には、各ポッドの境界リーフスイッチにルーティング可能な TEP アドレスが必要です。ルーティング可能な 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。それ以外の場合は、この項で説明されているように、Orchestrator GUI で TEP プールを追加できます。新しい TEP プールを追加する場合は、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ことに注意してください。

ステップ 1 Cisco ACI マルチサイト 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で、[スキーマ (schema)] を選択します。

ステップ 3 メインペインの右上にある [インフラの設定 (Configure Infra)] 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ルーティング可能な 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 ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] 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) 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。

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。

a) 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。

b) L3Out をインポートするサイトを選択します。

c) [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。

d) インポートする L3Out をチェックします。

e) [Import] をクリックします。

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 \(87 ページ\)](#) に説明されている方法で VRF と関連付けます。

ステップ 1 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 2 **[スキーマ (schema)]** を選択し、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 3 **[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 [eepg-intersite-l3out] 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。

ステップ 4 テンプレートレベルで L3Out を割り当てる場合...

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。

- a) 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。
- b) **[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。
- c) 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 5 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。

- a) 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。
- b) **[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。
- c) 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。

サイト間 L3Out のコントラクトの作成

ここでは、アプリケーション EPG とサイト間 L3Out を含む外部 EPG との間のトラフィックフローを有効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 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] を選択します。

ステップ 3 [スキーマ (schema)] 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。

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。

ステップ 4 コントラクトの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。
- 右側のサイドバーで、フィルタの[表示名 (Display Name)]を入力します。
- [エン트리 (Entry)] で [+エン트리 (+ Entry)] をクリックして、フィルタ エントリを入力します。
- [エントリの追加 (Add Entry)] ウィンドウで詳細を入力します。

作成するフィルタは、展開と許可するトラフィックのタイプによって異なります。

- [保存 (Save)] をクリックしてフィルタを保存します。

ステップ 5 コントラクトを作成します。

- [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。
- 右側のサイドバーで、コントラクトの[表示名 (Display Name)]を入力します。
- [範囲 (Scope)] ドロップダウンから、適切な範囲を選択します。

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。

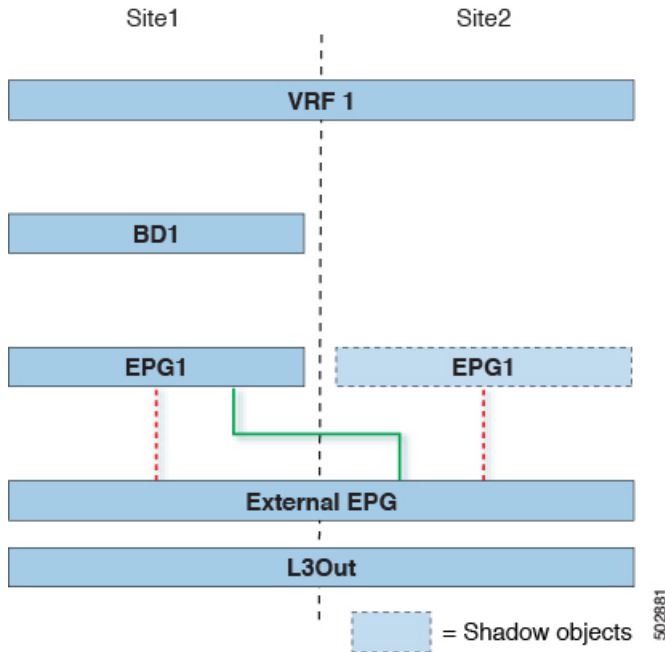
- [両方向に適用 (Apply Both Directions)] ノブをオンのままにします。
- [+フィルタ (+ Filter)] をクリックします。
- [名前 (Name)] ドロップダウン メニューから、前の手順で作成したフィルタを選択します。
- [保存 (Save)] をクリックして、フィルタをコントラクトに追加します。

アプリケーション EPG のサイト間 L3Out の設定

このセクションでは、別のサイトで L3Out を使用するようにアプリケーション EPG を設定する方法について説明します。

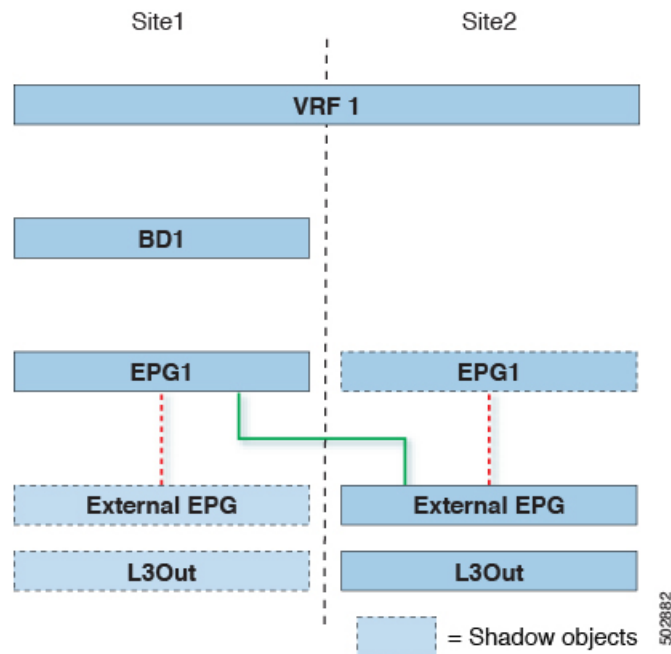
下の図に、拡大された外部 EPG と、両方のサイトで作成される関連づけられた L3Out を示します。アプリケーション EPG (epg1) はサイト 1 で作成され、外部 EPG とのコントラクトがあります。

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



L3Out を含む外部 EPG を拡張するかどうかにかかわらず、アプリケーション EPG と外部 EPG 間の通信はコントラクトによって有効になります。次の手順では、アプリケーション EPG を作成し、以前に設定した L3Out 外部 EPG との間でコントラクトを設定する方法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。

- [サイト間 L3Out を使用するための外部 EPG の設定 \(88 ページ\)](#) で説明されているように、サイト間 L3Out の外部 EPG。
- [サイト間 L3Out のコントラクトの作成 \(90 ページ\)](#) 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。
- サイト間 L3Out を使用するアプリケーション EPG。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] を選択します。

ステップ 3 アプリケーション EPG のスキーマを選択します。

ステップ 4 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。

- a) EPG を選択します。
- b) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
- c) 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。

ステップ 6 サイト間 L3Out を含む外部 EPG にコントラクトを割り当てます。

- a) 外部 EPG が配置されているテンプレートを参照します。
- b) 外部 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) 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。

ステップ 7 適切なサイトにテンプレートを割り当てます。

外部 EPG が拡張されている最初の図に示されている使用例を設定する場合は、外部 EPG のテンプレートをすべてのサイトに割り当て、アプリケーション EPG を 1 つのサイトに割り当てます。

外部 EPG とアプリケーション EPG がサイトに対してローカルである 2 番目の図に示されている使用例を設定する場合は、外部 EPG のテンプレートを 1 つのサイトに割り当て、アプリケーション EPG のテンプレートを別のサイトに割り当てます。

ステップ 8 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。

- a) 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。
- b) 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。
- c) 右側のサイドバーで、**[+ L3Out]** をクリックします。
- d) 作成したサイト間 L3Out を選択します。

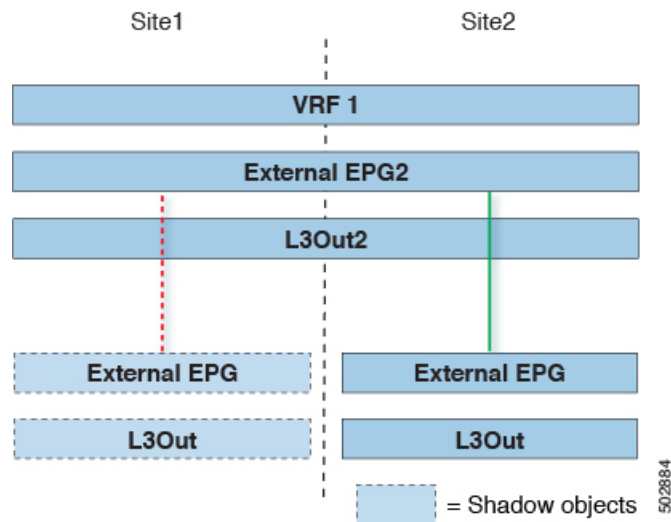
ステップ 9 スキーマを展開します。

サイト間での中継 L3Out の設定

このセクションでは、1 つのサイトの L3Out の背後にあるエンドポイントと、別のサイトの L3Out の背後にあるエンドポイント間の通信を設定する方法について説明します。

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 21: 中継 L3Out



この図は外部 EPG の 1 つを示していますが、もう一方はサイトローカルで、中継 L3Out は 3 つのすべての組み合わせをサポートしています。この場合、外部 EPG は拡大されず、どちらかが拡大されるか、または両方ともサイト間で拡大されます。

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。

- 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 (88 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 (90 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。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、[スキーマ (schema)] 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。

次を選択することができます

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。

- c) 外部 EPG を選択します。
- d) 右側のサイドバーで、[+コントラクト (+Contract)] をクリックします。
- e) 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。

ステップ 5 適切なサイトにテンプレートを展開します。

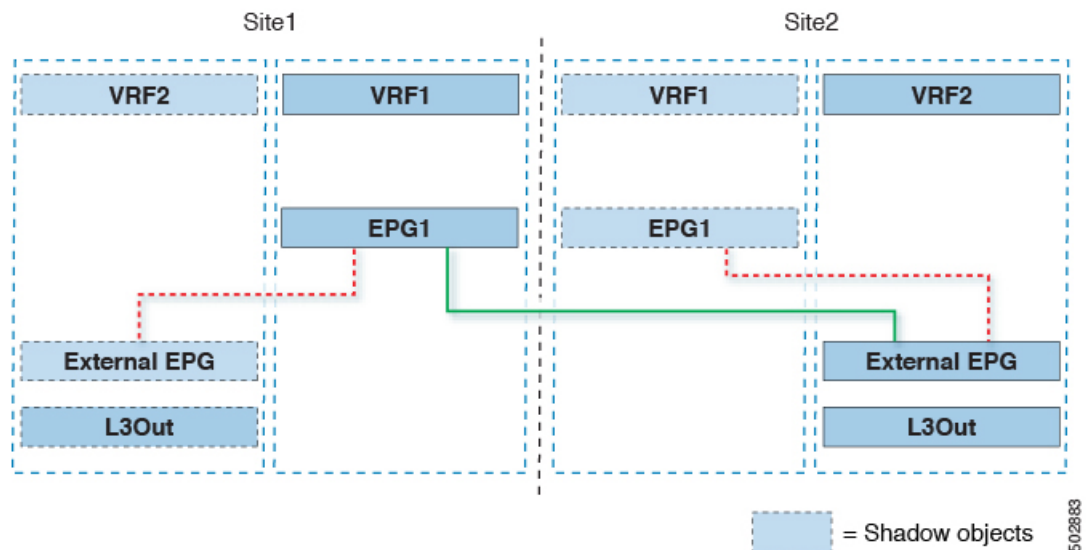
外部 EPG を1つのサイトまたは複数のサイトに展開することを選択できます。上の図は、1つの外部 EPG が1つのサイトのみに展開されている間に1つの外部を拡大する例を示していますが、外部 EPG に対してストレッチまたはサイトローカルを任意に組み合わせて選択することもできます。L3Outsは異なるサイトにあるため、トラフィックはサイト間で ACI ファブリックを通過します。

サイト間 L3Out による共有サービス

共有または中継サイト間 L3Out のための共有サービスの設定は、[アプリケーション EPG のサイト間 L3Out の設定 \(90 ページ\)](#) および [サイト間での中継 L3Out の設定 \(93 ページ\)](#) で説明している設定と類似していますが、下のように、いくつかの重要な相違点があります..

VRF 間の共有 L3Out

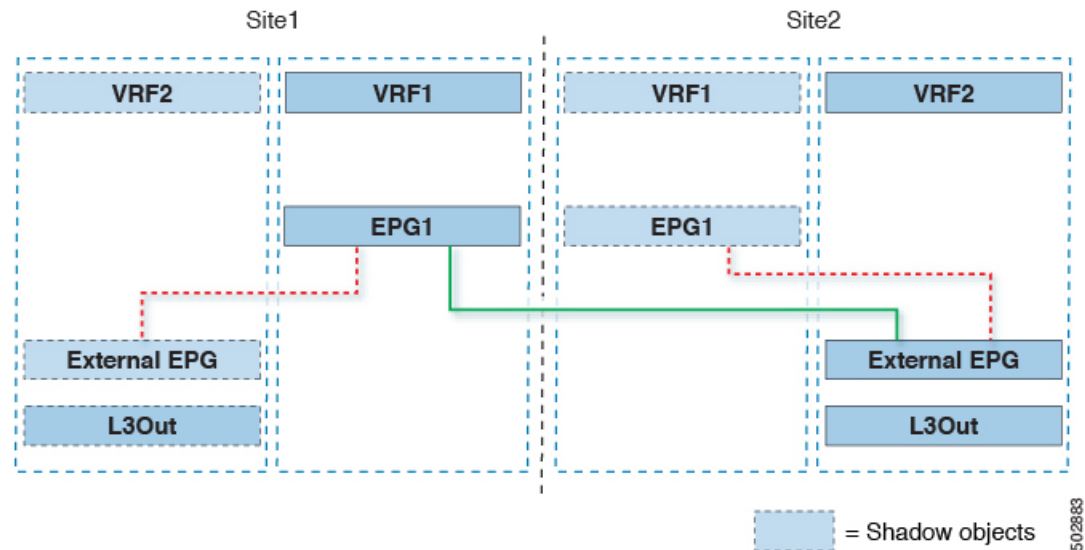
下の図はVRF 間の共有 L3Out シナリオの例を示しています。ここで、アプリケーション EPG (epg-1) は site1 内にあり、vrf-1 は site2 の L3Out を使用していますが、これは vrf-2 内にあります。



この VRF 間ユース ケースを設定する際には、アプリケーション EPG のブリッジドメインを設定するときに、[外部にアドバタイズ (Advertised Externally)] と [VRF 間で共有 (Shared Between VRF)] フラグを有効にする必要があります。

VRF 間の中継 L3Out

そして、下の図は、VRF 間の中継 L3Out シナリオの例を示しています。ここで、異なる VRF 内に位置する、2つの異なる L3Out を持つ2つの外部 EPG は、コントラクトで設定されています。



この VRF 間ユース ケースを設定する際には、外部 EPG のサブネットを設定するときに、[共有ルート制御サブネット (Shared Route Control Subnet)]、[共有セキュリティ インポート サブネット (Shared Security Import Subnet)]、および [共有ルートを集約 (Aggregate Shared Routes)] フラグを有効にする必要があります。

EPG 優先グループ

デフォルトでは、マルチサイト 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 マルチサイト 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、Multi-Site 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。

制限事項

優先グループはサイト間 L3Out 拡張外部 EPG でサポートされますが、サイトローカル 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 ACI マルチサイト 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マルチサイト 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 がマルチサイト 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。

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 マルチサイト 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、マルチキャストはすべての BD で無効になっています。

EPG が、拡張されていない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と、マルチサイト Orchestrator は、このような EPG ごとに、リモートサイトにシャドウ EPG を作成します。これにより、サブネットルートなどの設定変更がリモート トップオブブラック (TOR) スイッチにプッシュされる可能性があります。この点を軽減するため、レイヤ3マルチキャストは、マルチキャストの送信元が存在する、個々の EPG 上でも有効にする必要があります。その場合、それらの EPG で必要な設定だけが、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。

- あるサイトで、マルチキャストソースをエンドポイント (EP) として ACI ファブリックにアタッチした場合、そのサイトのスパインスイッチはマルチキャストトラフィックを別のサイトの送信します。ここでは、ソースの VRF は、ヘッドエンドレプリケーション (HREP) を使用してインスタンス化されます。マルチキャストトラフィックは VRF が拡張されている他のサイトに送り出され、マルチキャストトラフィックは、グループメンバーシップに基づいて出力リーフスイッチでプルーニング/転送されます。
- マルチキャストルーティングソリューションは、ランデブーポイント (RP) となる外部マルチキャストルータを必要とします。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、ファイブリック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。そのようなわけで、一方のサイトの L3Out を発するトラフィックは、別のサイトには送信されません。このことは、スパインにおいて、HREP トンネルへのレプリケーションから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す。
- 外部ルータから TOR の L3Out ブリッジドメインに入力されるマルチキャストトラフィックでは、外部 VXLAN ヘッダの特別な DSCP 値で、再マーキングが行われます。スパインでは、その DSCP 値のマッチングが行われ、HREP コピーを ISN ネットワークに複製して得られたすべてのマルチキャストトラフィックはプルーニングされます。
- あるサイトから送信されたトラフィックは、任意のサイトの L3Out から送信できます。
- BD とマルチサイト Orchestrator からの 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) を含めて、すべてのリーフスイッチにインジェクトされます。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 に対してポリシーが設定されていた場合、サブネットは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。L3Out ポリシーが、0/0 を含む大規模なサブネット範囲を許可しており、EPG でマルチキャストが有効になっていた場合、BD のサブネットとホストルートは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。

Layer 3 マルチキャストに関するガイドラインと制限事項

Cisco ACI マルチサイト Orchestrator は各サイトに必要なローカルポリシーを作成できません。そのため、エンドツーエンドのソリューションを機能させるために、各 APIC サイトで IGMP 関連ポリシー、PIM 関連ポリシー、ルートマップ、RP、および L3Outs を個別に設定する必要があります。

また、すべてのファブリックの DSCP 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。DSCP パケットヘッダー値は、サイト間で送信されるマルチキャストトラフィックに対して一致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 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。

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 フィルタ処理は、同じブリッジドメイン (BD) 内の複数の EPG ではサポートされていません。

マルチキャスト フィルタ処理はレイヤ 3 レベルで実行されるため、同じブリッジドメインに複数の EPGs を設定し、許可アクションを設定し、もう1つを [拒否 (Deny)] アクションとともに設定すると、レイヤ 3 マルチキャストはフィルタの対象を決定できなくなります。複数の EPG に対してマルチキャスト フィルタ処理を有効にする場合は、それらを個別の 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。送信元固有のマルチキャスト (SSM) 範囲をサポートしている

場合は、IGMPv3 を使用した SSM join itself で送信元と結合をフィルタ処理することを推奨します。

マルチキャスト フィルタ処理機能の SSM 範囲を設定する場合は、次の制約事項が適用されます。

- **送信元フィルタ処理に対する影響:** SSM ルートはすでにハードウェアのドロップ エントリとしてプログラムされているため、ファースト ホップ ルータ (fhr) ではパケットは受信されません。したがって、送信元フィルタ処理は SSM 範囲の影響を受けません。
- **受信者のフィルタ処理に適用:** 特定のブリッジ ドメインの最後のホップで受信した SSM join は、マルチキャスト RPF ルーティング情報ベース (MRIB) ルートでブロックされているように、そのグループの発信インターフェイス (OIF) リストを表示します。これは、最後のホップで IGMP のレポートポリシーを使用して実現することもできます。これにより、マルチキャスト ルーティング テーブルでの状態の作成が維持されます。
- 送信元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	操作
1	192.0.0.0/16	Permit
2	192.0.3.0/24	拒否 (Deny)

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。



(注) マッチングの順序は、送信元のフィルタリングにのみ適用されません。受信者フィルタリングの場合、順序は重要ではなく、最長一致ルールが適用されます。

レイヤ3 マルチキャストの有効化

以下の手順では、Cisco ACI マルチサイト Orchestrator GUI を使用して、VRF、BD、および EPG でレイヤ3 マルチキャストを有効にする方法を説明しています。

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 \(100 ページ\)](#) 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。

ステップ1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ2 左側のサイドバーから、[スキーマ (schema)] 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 VRF 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 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6 最後に、EPG でマルチキャストを有効にします。

いったん BD で L3 マルチキャストを有効にすると、マルチキャスト送信元を持つ EPG を選択できるようになります。これは、EPG がマルチキャストを有効にした BD または VRF の一部である場合にのみ行えます。

- 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) 右側のサイドバーで、[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 7 章

管理操作

- サイトのステータスの表示 (103 ページ)
- スキーマヘルスの表示 (103 ページ)
- 個々のサイトの障害の表示 (104 ページ)
- DHCP リレー ポリシー (105 ページ)
- システム ログ (113 ページ)
- 設定のバックアップと復元 (115 ページ)
- カスタム SSL 証明書 (122 ページ)
- 外部認証 (125 ページ)
- システム設定 (131 ページ)

サイトのステータスの表示

マルチサイト Orchestrator GUI のダッシュボードビューを使用して、各サイトのステータス、障害の数とタイプ、およびスキーマの健全性を表示できます。

[**サイトステータス (SITE STATUS)**] パネルでは、ダッシュボードに次のフィールドが表示されます:

- **SITE NAME** (サイト名)
- **CRITICAL Alarms** (緊急アラーム)
- **MAJOR Alarms** (メジャーアラーム)
- **MINOR Alarms** (マイナーアラーム)
- **WARNING Alarms** (警告アラーム)

スキーマヘルスの表示

マルチサイト Orchestrator GUI ダッシュボードのスキーマ健全性機能を使用すれば、さまざまなサイトに関連付けられている個々のスキーマの健全性を表示できます。 [**スキーマの詳細**

(Schema Details) ウィンドウでは、各サイトに関連付けられているポリシータイプを表示できます。

GUI の [スキーマヘルス (SCHEMA HEALTH)] チャートでは、以下のタスクを実行できます:

- マルチサイト ファブリック全体とすべて APIC の健全性スコアを集約して表示する
- [スキーマの詳細 (Schema Details)] ウィンドウで、集計されたエラー数と、スキーマごとのエラータイプを表示する
- サイト間スキーマの健全性を表示する
- 複数のサイト ノードとそのコンポーネントの健全性を表示する
- 接続された APIC および ACI クラスタの健全性を表示する

GUI では、以下のいくつかのフォーマットで、スキーマの健全性を表示できます:

- 個々のセルにマウスを合わせます。[スキーマヘルス (SCHEMA HEALTH)] チャートの各セルは、スキーマの健全性を示しています。セルが緑色で表示されている場合、マウスをそのセルに合わせると、スキーマのアプリケーション健全性が表示されます。
- セルをクリックします。テーブルの個々のセルをクリックすると、テンプレートに関するスキーマの詳細と、各ポリシータイプ (ANP、EPG、コントラクト、VRF、BD など) に関連付けられたエラーが表示されます。

エラーと警告は各ポリシーの右側の列に表示されます。この機能は、詳細を収集し、健全性を低下させている問題についてより多くの情報を得るために使用されます。

- 健全性スコア スライダの表示。ページの上にある健全性スコア スライダを使えば、健全性スコアの最小または最大に基づいてスキーマのフィルタリングを行えます。スライダによって範囲を調整すれば、健全性スコアの範囲に一致するスキーマを表示できます。たとえば、健全性スコアを調整して、0～30 の範囲内の健全性スコアに一致するスキーマを表示することができます。
- 検索機能を使用する。スキーマの健全性ビューの検索機能では、検索エリアに入力されたキーワードに基づいてスキーマまたはポリシーを見つけることができます。検索領域にキーワードを入力すると、キーワードを含むスキーマだけが表示されます。結果は、スキーマ名、テンプレート名、またはそのスキーマ内で含まれているポリシーのいずれかの一部として一致するキーワードに基づいています。

個々のサイトの障害の表示

ここでは、マルチサイト GUI を使用して個々のサイトの障害を表示する方法について説明します。

ステップ 1 マルチサイト Orchestrator GUI にログインします。

ステップ 2 **Main Menu** で **Sites** をクリックします。

ステップ 3 Sites list ページで **CONFIGURE INFRA** をクリックします。

ステップ 4 Fabric Connectivity Infra ページの **Master List** で、適切なサイトをクリックします。たとえば、site1 をクリックします。

サイトの詳細と、関連付けられているポッドとスパインが GUI に表示されます。

パネルの上部には、障害の総数と障害のタイプが表示されます。たとえば、タイプとしては、Critical、Major、Minor、および Warning があります。それぞれの障害のタイプをクリックすると、障害の詳細と、個々のコードおよびその説明が表示されます。

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 ext 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たびに、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が、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) DHCP ポリシーをブリッジドメインに割り当て、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には、各サイトの APIC で更新する DHCP ポリシーの変更を行うために、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

次のものがが必要です。

- 使用している環境でセットアップして設定された DHCP サーバ。
- DHCP サーバがアプリケーション EPG の一部となる場合は、[スキーマ管理 \(71 ページ\)](#) 章での説明に従って、その EPG がマルチサイト Orchestrator ですすでに作成されている必要があります。

DHCP サーバがファブリックの外部にある場合は、[スキーマ管理 \(71 ページ\)](#) 章での説明に従って、DHCP サーバへのアクセスに使用される L3Out に関連付けられている外部 EPG がすでに作成されている必要があります。

- ステップ 1** マルチサイト Orchestrator 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 (Policies)]** を選択します。
- ステップ 3** メイン ペインの右上にある **[ポリシーの追加 (Add Policy)]** をクリックし、**DHCP** を選択します。
[DHCP の追加 (Add DHCP)] 設定画面が表示されます。

- 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 (Select Tenant)]** 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 (Description)]** 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 (Type)]** として **[リレー (Relay)]** 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場合は、次の 2 つのタイプのいずれかを選択します。

- **[アプリケーション EPG (Application 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 (L3 External Network)]**: 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 で作成し、指定したテナントに割り当てられた EPG または外部 EPG は、サイトにまだ展開していない場合でも、選択することができます。展開されていない EPG を選択した場合でも、DHCP リレー設定を完了できます。ただし、リレーを使用できるようにするには、その前に 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 (DHCP Server Address)]** フィールドに、DHCP サーバの IP アドレスを入力します。

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。

追加する DHCP サーバごとに、ステップ 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。
- [スキーマ管理 \(71 ページ\)](#) 章の説明に従って、Multi-Site 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 \(107 ページ\)](#) 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 マルチサイト Orchestrator 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 (Policies)]** を選択します。

ステップ 3 メイン ペインの右上にある **[ポリシーの追加 (Add Policy)]** をクリックし、**DHCP** を選択します。

[DHCP の追加 (Add DHCP)] 設定画面が表示されます。

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 オプションを含めることができます。

- ステップ 5** [テナントの選択 (Select Tenant)] 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 (Description)] 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 (Type)] に対して [オプション (Option)] 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。
- どうしても必要というわけではありませんが、RFC 2132に記載されているオプションと同じ名前を使用することを推奨します。
- たとえば、[Name Server]などです。
- ステップ 10** オプションの ID を指定します。
- RFC 2132に記載されているオプション コードを指定する必要があります。
- たとえば、ネーム サーバ オプションの場合は 5 です。
- ステップ 11** オプションのデータを指定します。
- オプションで必要な場合は、値を入力します。
- たとえば、ネーム サーバ オプションで、クライアントが使用可能なネーム サーバのリストです。
- ステップ 12** オプションを保存するには、[データ (Data)] フィールドの横にあるチェックマークをクリックします。
- ステップ 13** (オプション) その他のオプションを追加するには、こ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

次のものがすでに設定されている必要があります。

- [DHCP リレー ポリシーの作成 \(107 ページ\)](#) 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 \(108 ページ\)](#) の説明に従って、DHCP オプション ポリシー。
- [スキーマ管理 \(71 ページ\)](#) 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** マルチサイト Orchestrator 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、[スキーマ (schema)] 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 \(108 ページ\)](#) 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ってフィルタリングされませんが、多くの場合、VRF 内および VRF 間でルーティング情報を伝搬するためにコントラクトが必要です。DHCP パケットがフィルタリングされない場合でも、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ている EPG との間では、コントラクトを設定することを推奨します。

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 ポリシーをすでに作成して、ブリッジドメインと、クライアントの EPG へのブリッジドメインに割り当てている場合でも、クライアントからサーバへの通信を可能にするために、ルートのプロゲラミングを有効にするコントラクトを作成して割り当て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。

- [DHCP リレーポリシーの作成 \(107 ページ\)](#) 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 \(108 ページ\)](#) 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 \(109 ページ\)](#) 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** マルチサイト Orchestrator 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、[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する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ないため、特定のフィルタは必要ありませんが、適切な BD とルートの展開を保証するために、有効なコントラクトを作成して割り当てる必要があります。

- 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) 右側のサイドバーで、コントラクトの**[表示名 (Display Name)]**を入力します。
- c) **[範囲 (Scope)]** ドロップダウンから、適切な範囲を選択します。

DHCP サーバの EPG とアプリケーション EPG は同じテナント内にある必要があるため、次のいずれかを選択できます。

- [vrf](両方の EPG が同じ VRF にある場合)
- [テナント (tenant)](EPG が異なる VRF にある場合)

- d) **[両方向に適用 (Apply Both Directions)]** ノブは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) DHCP サーバが存在する EPG または外部 EPG を選択します。

これは、DHCP リレー ポリシーの作成時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、そのタイプのため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) 作成した契約と、そのタイプのため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、Multi-Site Orchestrator 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 マルチサイト Orchestrator 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 (Policies)**] 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。

システム ログ

マルチサイト Orchestrator システム ロギングは、最初に Orchestrator クラスタを展開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。

マルチサイト Orchestrator 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 **[管理 (Admin)]** > **[監査ログ (Audit logs)]** を選択します。

[監査ログ (Audit Logs)] ページで、**[最新 (Most Recent)]** 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):** ポリシー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ます。たとえばサイト、ユーザ、テンプレート、アプリケーションプロファイル、ブリッジドメイン、EPG、外部EPG、フィルタ、VRF、BGP設定、契約、OSPFポリシー、ポッド、ノード、ポート、ドメイン、プロバイダは、RADIUS、TACACS+ をクリックして、**[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 **[適用 (Apply)]** をクリックします。

トラブルシューティング レポートとログの生成

このセクションでは、Cisco ACI マルチサイト 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 マルチサイト Orchestrator GUI にログインします。

ステップ 2 右上隅で、**[オプション (Options)]** アイコンをクリックして、**[システム ログ (System Logs)]** をクリックします。

ステップ 3 ダウンロードするログを確認します。

[データベースのバックアップ (Database Backup)] をクリックして、Orchestrator データベースのバックアップをダウンロードします。

[サーバ ログ (Server Logs)] をチェックして、Orchestrator ログをダウンロードします。

ステップ4 [ダウンロード (DOWNLOAD)] をクリックします。

選択した項目のアーカイブがシステムにダウンロードされます。このレポートには、次の情報が含まれています。

- JSON フォーマットでのすべてのスキーマ
- JSON フォーマットでのすべてのサイト定義
- JSON フォーマットでのすべてのテナント定義
- JSON フォーマットでのすべてのユーザ定義
- infra_logs.txt ファイル内のテナントのすべてのログ

外部ログアナライザへのログストリーミングを有効にする

Cisco ACI マルチサイト Orchestrator を使用すると、Orchestrator ログを外部のログアナライザ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し、表示し、それらに対応できます。

ここでは、マルチサイト Orchestrator が外部アナライザツール (Splunk 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

- ログアナライザ 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。



(注) Cisco ACI マルチサイト Orchestrator の本リリースでは、サービスプロバイダとして Splunk のみがサポートされています。

- サービスプロバイダの認証トークンを取得します。
分裂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、簡単に言うと、[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 マルチサイト Orchestrator GUI にログインします。

ステップ2 右上隅で、[オプション (Options)] アイコンをクリックして、[システム ログ (System Logs)] をクリックします。

- ステップ3** 開いた [システムログ (System Logs)] ウィンドウで、[外部ストリーミング (EXTERNAL STREAMING)] ノブを有効にします。
- ステップ4** ストリーミングするログを選択します。
- [すべてのログ (all logs)] または [監査ログのみ (audit log only)] のいずれかを選択できます。
- ステップ5** [サービスの選択 (SELECT SERVICE)] ドロップダウンメニューから、ログアナライザサービスを選択します。
- このリリースの Cisco ACI マルチサイト Orchestrator では、サービスプロバイダとして Splunk のみがサポートされています。
- ステップ6** トラフィックの [プロトコル (PROTOCOL)] を選択します。
- HTTP の場合には [非セキュア (UNSECURE)]、HTTPS の場合には [セキュア (SECURE)] を選択します。
- ステップ7** サービスの情報を入力します。
- [ホスト (HOST)] フィールドに、ホストの IP アドレスを入力します。
- [ポート (PORT)] フィールドに、ポート番号を入力します。
- [トークン (TOKEN)] フィールドに、サービスプロバイダから取得した認証トークンを入力します。
- ステップ8** マルチサイト Orchestrator ノードごとに、ノードのルートパスワードを入力します。
- (注) これは、Orchestrator GUI へのログインに使用するパスワードではなく、各 Orchestrator ノードのルートユーザパスワードです。
- ステップ9** [OK] をクリックして変更を保存します。

設定のバックアップと復元

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ために、マルチサイト 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、および各設定の変更または展開後には、設定のバックアップを作成することを推奨します。また、Orchestrator ノードの VM の外部にある外部ストレージにバックアップをエクスポートすることをお勧めします。



- (注) バックアップアクションの復元は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースには変更を加えません。したがって、Orchestrator データベースを復元した後で、Orchestrator と APIC サイト間のポリシーが食い違う可能性を避けるため、既存のスキーマを再展開する必要もあります。特定の設定が食い違うシナリオと、それぞれに関連するバックアップ復元手順の詳細については、次を参照してください。[バックアップと復元に関するガイドライン \(116 ページ\)](#)
-

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。

- 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、展開されていないポリシーは「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は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースに変更を加えません。そのため、以下で説明するように、以前の設定を復元して、Orchestrator と APIC サイトの間でポリシーが一致しない可能性を回避するために、特定の注意事項と手順を実行する必要があります。

バックアップ以降の設定変更がない場合

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。[バックアップの復元 \(121 ページ\)](#) 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、APIC サイトのオブジェクトやポリシーは変更されません。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。古い設定を回避するには、バックアップを復元した後に手動でこれらを削除する必要があります。

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、古いオブジェクトが残る可能性を回避されます。ただし、この操作により、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 \(121 ページ\)](#) で説明しています。
- 復元した設定バックアップが APIC サイトに展開される前に保存された場合は、「未展開」状態で復元され、必要に応じて APIC サイトに展開できます。
- 設定がすでに展開されているときに復元した設定バックアップが保存された場合、APIC サイトにまだ存在していないポリシーがあっても、「展開済み」状態で復元されます。この場合、設定を各サイトに適切にプッシュするには、いくらかの設定変更をして、それを再展開して、Orchestrator の設定を APIC サイトと同期させる必要があります。

リモートバックアップ

Cisco ACI マルチサイトは、3 ノードのクラスタとして展開されます。クラスタを最初に展開すると、作成したバックアップは、`/opt/cisco/msc/backups/`ディレクトリ内の各ノードのローカルディスク上に配置されているデフォルトの場所に保存されます。

バックアップは任意の1つのノードで使用でき、Orchestrator GUI を使用して表示できますが、Orchestrator VM の外部にあるリモートロケーションにすべてのバックアップをエクスポートすることを推奨します。すべての Orchestrator バックアップに対してリモートロケーションを設定するには、次の2つの方法があります。

- リモート NFS 共有を設定し、各ノードのデフォルトのバックアップディレクトリにマウントします。その場合、バックアップファイルは、Orchestrator VM のローカルドライブをバイパスするリモート NFS 共有に直接書き込まれます。

このアプローチでは、Orchestrator GUI から作成されたすべての設定バックアップに1つのリモートロケーションのみを使用できるため、柔軟性が低くなります。

- Orchestrator 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、そこでバックアップファイルをエクスポートします。

リモート NFS 共有アプローチとは異なり、Orchestrator GUI で1つ以上のリモートロケーションを設定すると、複数の宛先を指定して、バックアップファイルを保存できる場所に柔軟性を高めることができます。



(注) 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、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。ローカルバックアップのディスク領域の使用には制限があります。これに達すると、リモートバックアップの作成が妨げられる可能性があります。

バックアップのリモートロケーションの設定

ここでは、設定バックアップをエクスポートできるマルチサイト Orchestrator でリモートロケーションを設定する方法について説明します。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーションウィンドウで、**[管理 (Admin)] > [リモートロケーション (Remote Locations)]** 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 ロケーションの名前と説明 (任意) を入力します。

既存のバックアップをリモート ロケーションへ移動する

現在、設定バックアップのリモート エクスポートでは、次の2つのプロトコルがサポートされています。

- SCP
- SFTP

ステップ5 リモート サーバのホスト名または 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 バックアップを保存するリモート サーバ上のディレクトリへのフルパスを指定します。

パスはスラッシュ (/) 文字で始まる必要があり、ピリオド (.) またはバックスラッシュ (\) を含めることはできません。たとえば、`/backups/multisite`などです。

(注) ディレクトリはすでにリモート サーバに存在している必要があります。

ステップ7 リモート サーバへの接続に使用するポートを指定します。

デフォルトでは、ポートは22に設定されています。

ステップ8 リモート サーバに接続するとき使用する認証タイプを指定します。

次の2つの認証方式のいずれかを設定できます。

- パスワード: リモート サーバにログインするために使用す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: リモートサーバへのログインに使用するユーザ名と SSH キー/パスフレーズ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。

既存のバックアップをリモート ロケーションへ移動する

このセクションでは、マルチサイト Orchestrator GUI で作成した既存の設定バックアップを、ノードのローカル ドライブからリモート ロケーションに移動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 \(120ページ\)](#) 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。
- [バックアップのリモートロケーションの設定 \(117ページ\)](#) の説明に従って、バックアップをエクスポートするためのリモート ロケーションが追加されていること。

ステップ1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ2 左側のナビゲーションウィンドウで、[管理 (Admin)] > [バックアップ (Backups)] を選択します。

ステップ 3 エクスポートするバックアップを見つけて、その横にあるアクション()アイコンをクリックし、[リモート ロケーションへ移動 (Move to remote location)] をクリックします。

[バックアップをリモート ロケーションに移動 (Move Backup To Remote Location)] ウィンドウが開きます。

ステップ 4 [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 5 (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。

Adding an NFS Share to Store Backups

ここでは、設定のバックアップを保存するために、マルチサイト Orchestrator VM に NFS 共有を追加する方法について説明します。



(注) 設定のバックアップには単一のリモート NFS 共有を設定できますが、Orchestrator GUI で使用可能なリモートバックアップロケーション機能を使用することをお勧めします。代わりに、[バックアップのリモートロケーションの設定 \(117 ページ\)](#) で説明します。

ステップ 1 ルートユーザとして、マルチサイト Orchestrator ノードの VM に直接ログインします。

ステップ 2 NFS 共有をマウントします。

次のコマンドは、共有 NFS ディレクトリをデフォルトの Orchestrator バックアップ フォルダにマウントします。これにより、将来のすべてのバックアップは、Orchestrator VM 外の外部ストレージに自動的に保存されます。

(注) 保存するデフォルトディレクトリに既存のバックアップがある場合は、NFS 共有をマウントする前に、それらを手動で別の場所に移動する必要があります。共有がマウントされると、マウントディレクトリ内の既存のファイルは表示されなくなります。

```
# mount <nfs-server-ip>:<nfs-share-path> /opt/cisco/msc/backups/
```

ステップ 3 各 Orchestrator VM でステップ 1~2 を繰り返します。

各 Orchestrator ノードは独自のバックアップ ファイルを作成して保存できるため、すべてのノードに同じ NFS 共有をマウントする必要があります。

ステップ 4 Docker バックアップ サービスを更新します。

新しくマウントされたファイル システムを Orchestrator サービスで使用可能にするには、次の Docker 更新コマンドを実行する必要があります。ただし、コマンドによってクラスタ全体のサービスが更新されるため、各ノードに共有をマウントした後にこの操作を実行する必要があるのは1回だけです。

```
# docker service update msc_backupservice --force
```

次のタスク

いずれかの時点でNFS共有を削除して、各VMにローカルにバックアップを保存する場合は、各ノードのディレクトリをアンマウントして、`docker service update msc_backupservice--force` コマンドを再度実行します。

バックアップの作成

このセクションでは、マルチサイト 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

リモート ロケーションを使用してバックアップを作成する場合は、最初に [バックアップのリモートロケーションの設定 \(117ページ\)](#) の説明に従ってリモート ロケーションを追加する必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーションウィンドウで、**[管理 (Admin)] > [バックアップ (Backups)]** を選択します。

ステップ 3 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。

ステップ 4 **[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。

ステップ 5 (オプション) **[注 (Notes)]** フィールドに、バックアップについての追加情報を入力します。

ステップ 6 **[バックアップの場所 (Backup Location)]** を選択します。

バックアップファイルは、Orchestrator ノードにローカルに保存するか、またはリモート ロケーションにエクスポートすることができます。

バックアップ ファイルをローカルに保存する場合は、**[ローカル (Local)]** を選択します。

それ以外で、バックアップ ファイルをリモートの場所に保存するには、**[リモート (Remote)]** を選択して次の情報を入力します。

- **[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。

- **[リモートパス (Remote Path)]**では、デフォルトのターゲットディレクトリのままにするか、またはパスに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 [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、マルチサイト 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

バックアップアクションの復元は、マルチサイト Orchestrator でのデータベースを復元しますが、各サイトの APIC データベースには変更を加えません。したがって、Orchestrator データベースを復元した後で、Orchestrator と APIC サイト間のポリシーが食い違う可能性を避けるため、既存のスキーマを再展開する必要もあります。

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 \(116 ページ\)](#) を参照してください。

ステップ1 マルチサイト Orchestrator 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 \(116 ページ\)](#) 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、**[管理 (Admin)] > [バックアップ (Backups)]** 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、実行中のマルチサイト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。

ステップ6 必要に応じて、設定を再展開します。

復元された設定を APIC サイトと同期するには、この手順を実行することをお勧めします。追加のコンテキストは、[バックアップと復元に関するガイドライン \(116 ページ\)](#) にあります。

バックアップのダウンロード

ここでは、マルチサイト 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 マルチサイト Orchestrator 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[管理者(Admin)] > [バックアップ(Backups)]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 `mssc-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。

バックアップのインポート

ここでは、マルチサイト Orchestrator に既存のバックアップをインポートする方法について説明します。

始める前に

ステップ 1 マルチサイト Orchestrator 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[管理者(Admin)] > [バックアップ(Backups)]を選択します。

ステップ 3 メインウィンドウで、[インポート(Import)]をクリックします。

ステップ 4 [ファイルからインポート(import from file)]ウィンドウが開いたら、[ファイルの選択(Select file)]をクリックして、インポートするバックアップファイルを選択します。

バックアップをインポートすると、[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そのバックアップが追加されます。

カスタム SSL 証明書

Cisco ACI マルチサイト Orchestrator OVA は、Orchestrator のインストール中に各ノードの `/data/mssc/secrets` ディレクトリに保存された事故署名付きの SSL 証明書を含みます。デフォルトで、Orchestrator GUI は HTTPS 接続に対してこの証明書を使用します。

Orchestrator ノードサーバーに直接ログインして、そのウェブサーバー(nginx)構成を変更することでこれらの証明書をあらかじめ更新できましたが、Cisco ACI マルチサイト Orchestrator リ

リリース 2.1(1)以降、GUIを使用して、Orchestrator の GUI 接続に使用されるカスタム証明書を簡単に追加または更新できます。

カスタム証明書を追加するときに、次の 2 つのオプションの 1 つを使用できます。

- **自己署名付き証明書** は、Orchestrator の GUI により使用される独自のパブリックとプライベート キーを作成する機能を付与します。
- **CA 発行証明書** は、既存の認証局 (CA) とそのキーにより提供された証明書を使用できません。

GUI でパブリック/プライベートキーの組み合わせを含む複数の CA とキーリングを追加できますが、一度にアクティブにできるのは 1 つのキーリングのみで、Orchestrator GUI とブラウザ間の通信を保護するために使用できます。

カスタム認証局の追加

HTTPS トラフィックの暗号化のために Orchestrator によって提供されるパブリック キーを検証するために使用されるカスタム認証局 (CA) を追加できます。

このセクションでは、マルチサイト Orchestrator GUI でカスタム CA を追加し、設定する方法について説明します。キーリングとキーの設定については、次のセクションで説明します。

ステップ 1 マルチサイト Orchestrator 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 **[管理者(Admin)] > [セキュリティ(Security)]** を選択します。

ステップ 3 メイン ウィンドウで、**[認証局 (Certificate Authority)]** タブを選択し、**[認証局の追加 (Add Certificate Authority)]** をクリックします。

ステップ 4 開いた **[認証局の追加 (Add Certificate Authority)]** ウィンドウで、CA の詳細を指定します。

[名前 (Name)] フィールドに、認証局の名前を入力します。

[説明 (Description)] フィールドに、説明を入力します。

[証明書チェーン (Certificate Chain)] フィールドに、CA の証明書チェーンを入力します。中間証明書とルート証明書の両方を含める必要があります。中間証明書を最初に入力し、その後にルート証明書を入力する必要があります。

ステップ 5 **[保存 (Save)]** をクリックして、変更内容を保存します。

カスタム キーリングの追加

Orchestrator GUI の HTTPS トラフィックの暗号化に使用される公開キーと秘密暗号キーを含むカスタムキーリングを追加できます。

ここでは、カスタム キーリングを追加する方法について説明します。このキーリングで公開キーの確認に使用できる認証局 (CA) を追加する手順については、前のセクションを参照してください。

-
- ステップ 1** マルチサイト Orchestrator 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 **[管理者(Admin)] > [セキュリティ(Security)]** を選択します。
- ステップ 3** メインウィンドウで、**[キーリング (Key Rings)]** タブを選択し、**[キーリングの追加 (ADD KEY RING)]** をクリックします。
- ステップ 4** **[キーリングの作成 (Create Key Ring)]** ウィンドウが開くので、キーリングの詳細を入力します。
- [認証局の選択 (SELECT CERTIFICATE AUTHORITY)]** ドロップダウンメニューから、キーリングを含む認証局を選択します。
- [名前 (Name)]** フィールドに、キーリングの名前を入力します。
- [キーリングの説明 (KEY RING DESCRIPTION)]** フィールドに、キーリングの説明を入力します。
- [公開キー (PUBLIC KEY)]** フィールドに、リングの公開キーを入力します。
- [秘密キー (PRIVATE KEY)]** フィールドに、リングの秘密キーを入力します。
- ステップ 5** **[保存 (Save)]** をクリックして、変更内容を保存します。
-

カスタムキーリングのアクティブ化

前のセクションで説明したようにキーリングを追加した後、デフォルトのキーリングとしてアクティブ化する必要があります。

-
- ステップ 1** マルチサイト Orchestrator 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 **[管理者(Admin)] > [セキュリティ(Security)]** を選択します。
- ステップ 3** メインウィンドウで、**[キーリング (Key Rings)]** タブを選択します。
- ステップ 4** メインウィンドウで、アクティブにするキーリングの横にある **[...]** アイコンをクリックし、**[キーリングをアクティブにする (Make Keyring Active)]** を選択します。
- ステップ 5** キーリングをアクティブにするには、**[アクティベート (ACTIVATE)]** をクリックします。
- キーをアクティブにすると、マルチサイト Orchestrator GUI からログアウトされます。ログインページがロードされると、新しい証明書とキーが使用されます。
-

カスタム証明書のトラブルシューティング

ここでは、マルチサイト Orchestrator でカスタム SSL 証明書を使用する場合の一般的な問題を解決する方法について説明します。

Orchestrator GUI をロードできません

カスタム証明書をインストールしてアクティブ化した後に Orchestrator GUI ページをロードできない場合は、各 Orchestrator ノードに証明書が正しくコピーされていない可能性があります。この問題を解決するには、デフォルトの証明書を回復してから、新しい証明書のインストール手順を再度繰り返します。

デフォルトの Orchestrator 証明書を回復するには、次のようにします。

1. 各 Orchestrator ノードに直接ログインします。
2. 証明書ディレクトリに移動します。

```
# cd /data/msc/secrets
```
3. msc.key ファイルと msc.cert ファイルを、それぞれ msc.key_backup ファイルと msc.cert_backup ファイルに置き換えます。

```
# cp msc.key_backup msc.key
# cp msc.cert_backup msc.cert
```
4. Orchestrator GUI サービスを再起動します。

```
# docker service update msc_ui --force
```
5. 前のセクションで説明したように、新しい証明書を再インストールしてアクティブにします。

クラスタへの新しい Orchestrator ノードの追加

マルチサイト Orchestrator クラスタに新しいノードを追加する場合は、次のようにします。

1. Orchestrator GUI にログインします。
2. 前のセクションで説明したように、使用しているキーを再度アクティブにします。

外部認証

RADIUS、TACACS+、LDAP サーバを使用して、外部ユーザ認証と認可を設定できます。

マルチサイト Orchestrator 管理者は、次のことができます。

- 1 つ以上の外部認証プロバイダを追加します。

冗長性のために、少なくとも 2 つの認証プロバイダを設定することをお勧めします。
- ログイン ドメインを作成し、プロバイダに関連付けます。

デフォルト ドメインは、ローカル認証のためのローカル ドメインです。
- ユーザをドメインに割り当てます。

ドメインを作成した後、ドメインの編集、非アクティブ化または削除を行えます。ローカルドメインを削除することはできませんが、非アクティブにすることはできます。

監査ログは、外部認証と承認をサポートします。

外部認証サーバの設定に関するガイドライン

マルチサイトOrchestrator ユーザ認証用の外部認証サーバを設定する場合は、次のようにします。

- リモート認証サーバーのユーザごとに設定を行う必要があります。
- 各ユーザに対して、そのユーザに割り当てられた使用権限(ロール)を指定して、カスタム属性値 (AV) ペアを追加する必要があります。ロールについては、[ユーザ、ロール、および権限 \(65 ページ\)](#)に記載されています。

ロールを指定する場合は、次の形式を使用します。

```
cisco-av-pair=shell:misc-roles=role1,role2
```

次に例を示します。

```
cisco-av-pair=shell:misc-roles=siteManager, schemaManager.
```

- リリース 2.1 (2) 以降では、各ユーザ ロールを読み取り専用モードで割り当てることができます。読み取り専用権限が付与されている場合、ユーザは以前と同様に、そのロールで使用可能な任意のファブリックオブジェクトを表示できますが、それらのオブジェクトに変更を加えることはできません。

AV ペアの文字列形式は、特定のユーザに読み取り専用または読み取り専用のロールを設定する場合に異なります。次の例では、読み取り/書き込みロールはスラッシュ (/) 文字を使用して読み取り専用ロールから分離されていますが、個々のロールはパイプ (|) 文字で区切られています。

```
cisco-av-pair=shell:misc-roles=writeRole1|writeRole2/readRole1|readRole2
```

次の例は、スキーマ マネージャとユーザ マネージャのロールをユーザに割り当てる方法を示していますが、サイトマネージャのユーザに表示されるオブジェクトを表示することもできます。

```
shell:misc-roles=schemaManager|userManager/siteManager
```

ユーザの読み取り専用権限または読み取り/書き込み権限のみを設定する場合は、スラッシュ (/) 文字を含める必要があります。次の例は、**Site Manager** ロールで使用可能なオブジェクトへの読み取り/書き込みアクセスまたは読み取り専用アクセスを設定する方法を示しています。

- 読み取り専用: `shell:misc-roles=/sitemanager`
- 読み取り/書き込み: `shell:misc-roles=sitemanager/`



(注) 古い(カンマ区切り)書式または新しい(パイプとスラッシュ)書式のどちらでもサポートされていますが、単一のユーザを設定するときにそれらを混在させることはできません。混在または不適切に書式設定された AV 文字列は解析されず、ユーザ ロールは設定されていません。

- 読み取り専用ユーザ ロールを設定してから、マルチサイト Orchestrator を以前のバージョンにダウングレードした場合、読み取り専用権限はサポートされません。これらのロールは、すべてのユーザから削除されます。これは、読み取り専用ロールのみを持つすべてのユーザにロールが割り当てられず、削除されることも意味します。パワーユーザまたはユーザ マネージャは、ユーザを再度作成し、新しい読み取り/書き込みロールを割り当てる必要があります。
- LDAP 設定のベストプラクティスは、属性文字列として **CiscoAVPair** を使用することです。何らかの理由で、オブジェクト ID 1.3.6.1.4.1.9.22.1 を使用できない場合は、追加のオブジェクト ID 1.3.6.1.4.1.9.2742 を使用できません。1-5は、LDAP サーバでも使用できません。

RADIUS または TACACS+ を認証プロバイダとして追加する

このセクションでは、Cisco ACI マルチサイト Orchestrator ユーザを認証するための外部認証サーバとして 1 つ以上の RADIUS または TACACS+ サーバを追加する方法を説明します。

- ステップ 1** ローカルドメインを使用して、Cisco ACI マルチサイト Orchestrator に admin ユーザとしてログインします。
- ステップ 2** 左側のナビゲーション ペインから [管理 (Admin)] > [プロバイダ (Provider)] を選択します。
- ステップ 3** メインウィンドウで、[プロバイダの追加 (Add Provider)] をクリックします。
- ステップ 4** 外部認証サーバのホスト名または IP アドレスを入力します。
- ステップ 5** (オプション) 追加するプロバイダの説明を入力します。
- ステップ 6** 追加するプロバイダ タイプとして、[RADIUS] または [TACACS +] を選択します。
- ステップ 7** [キー (KEY)] フィールドにキーを入力し、[キーの確認 (CONFIRM KEY)] フィールドでそれを確認します。
- ステップ 8** (オプション)。追加設定を行います。
 - a) [Additional Settings (追加設定)] を展開して、詳細設定を行います。
 - b) 認証サーバに接続するために使用されるポートを指定します。

デフォルトのポートは、**RADIUS** の場合は 1812、**TACACS +** の場合は 49 です。
 - c) 使用するプロトコルを指定します。

[PAP] プロトコルと [CHAP] プロトコルのいずれかを選択します。

- d) 認証サーバに接続する際のタイムアウトと試行回数を指定します。

LDAP を認証プロバイダとして追加する

このセクションでは、Cisco ACI マルチサイト Orchestrator ユーザを認証するための外部認証サーバとして1つ以上の LDAP サーバを追加する方法を説明します。

ステップ 1 ローカルドメインを使用して、Cisco ACI マルチサイト Orchestrator に admin ユーザとしてログインします。

ステップ 2 左側のナビゲーション ペインから **[管理 (Admin)] > [プロバイダ (Provider)]** を選択します。

ステップ 3 メインウィンドウで、**[プロバイダの追加 (Add Provider)]** をクリックします。

ステップ 4 外部認証サーバのホスト名または IP アドレスを入力します。

ステップ 5 (オプション) 追加するプロバイダの説明を入力します。

ステップ 6 追加する追加するプロバイダのタイプとして、**[LDAP]** を選択します。

ステップ 7 LDAP サーバの **[ベース DN (Base DN)]**、**[バインド DN (Bind DN)]**、および **[キー (Key)]** 値を入力します。

ベース DN とバインド DN は、LDAP サーバがどのように設定されているかに応じて決まります。ベース DN とバインド DN 値は、LDAP サーバで作成されたユーザの識別名から取得できます。

ベース DN は、サーバがユーザを検索するポイントです。たとえば、DC = mso, DC = local のようになります。

バインド DN は、サーバに対する認証に使用されるクレデンシャルです。たとえば、CN = admin, CN = Users, DC = mso, DC = local のようになります。

バインド DN には、次のフィールドに入力できるキーを付属させます。

ステップ 8 (オプション) LDAP 通信で SSL を有効にします。

- [有効 (Enabled)]** チェックボックスをオンにします。
- 使用する証明書を選択します。
- 検証レベルを選択します。

[許可 (Permissive):] 任意の認証局 (CA) によって署名された証明書を受け入れ、暗号化に使用します。

[制限あり (Restrictive):] 使用する前に証明書チェーン全体を確認します。

ステップ 9 (オプション)。追加設定を行います。

- [追加設定 (Settings)]** をクリックして展開します。
- LDAP サーバに接続するポートを指定します。

LDAP のデフォルトのポートは 389 です。

- 認証サーバに接続する際のタイムアウトと試行回数を指定します。
- 使用するフィルタを指定します。

フィルタ値はLDAPサーバの設定によって異なります。デフォルトのLDAPフィルタは (cn = username) です。ただし、Microsoft LDAP サーバを使用している場合は、代わりにフィルタを (sAMAccountName = {username}) に設定します。

e) 認証タイプを指定します。

認証タイプは次のとおりです。

- **[Cisco AVPair]:** 属性値 (AV) ペアを使用して、個々のユーザのロールに基づいて認可を設定します。この方法を使用する場合は、**[属性 (Attribute)]** フィールドを [Ciscoavpair] に設定します。また、次の形式で AV ペア文字列を使用して、LDAP サーバで各ユーザを個別に設定する必要があります。

- リリース 2.1(2) 以降:

```
cisco-av-pair=shell:misc-roles=writeRole1|writeRole2/readRole1|readRole2
```

- リリース 2.1(1) 以前:

```
cisco-av-pair=shell:misc-roles=role1,role2
```

詳細については、[外部認証サーバの設定に関するガイドライン \(126 ページ\)](#) を参照してください。

- **[LDAP グループマッピングルール (LDAP Group Map Rules)]:** LDAP サーバグループを使用して、ユーザのグループメンバシップに基づいて許可を設定します。この方法を使用する場合は、**[属性 (Attribute)]** フィールドを [memberOf] に設定し、**[+LDAP グループマッピングルール (+LDAP group Map Rules)]** をクリックしてグループメンバシップを指定します。

[新しいグループマッピングルール (New Group Map Rule)] で、グループ DN と (たとえば、CN=group1,OU=misc-ou,DC=misc,DC=local)、そのグループに割り当てられるユーザロールを指定します。同じグループマッピングルールに複数のロールを追加できます。各ユーザロールの詳細な説明については、[ユーザ、ロール、および権限 \(65 ページ\)](#) を参照してください。

ログインドメインの作成

ログインドメインは、ユーザの認証ドメインを定義します。ログインドメインは、ローカル、RADIUS、TACACS+、または LDAP 認証メカニズムを設定できます。

GUI を使用して Cisco ACI マルチサイト Orchestrator にログインする場合には、ユーザが選択できるよう、ログイン画面にドメインのドロップダウンリストが表示されます。ドメインを指定しなかった場合は、ローカルドメインがユーザ名の検索のために使用されます。

REST API を使用して Cisco ACI マルチサイト Orchestrator にログインする場合には、POST メッセージのログイン情報とともにログインドメインが指定されます。たとえば、次のようになります。

```
{
  "username": "bob",
  "password": "Welcome2misc!",
}
```

```
"domainId":"59d5b5978d0000d000909f65"  
}
```

Cisco ACI マルチサイト Orchestrator GUI でログインドメインを作成するには、次の手順に従います。

始める前に

[RADIUS または TACACS+ を認証プロバイダとして追加する \(127 ページ\)](#) または [LDAP を認証プロバイダとして追加する \(128 ページ\)](#) で説明されているように、1 つ以上の認証プロバイダを追加しておく必要があります。

ステップ 1 Cisco ACI マルチサイト 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)] > [ログインドメイン(Login Domains)]** を選択します。

ステップ 3 メインウィンドウで、**[ログインドメインの追加 (ADD LOGIN DOMAIN)]** をクリックします。

ステップ 4 ドメイン名を入力します。

ステップ 5 (オプション) ドメインの説明を入力します。

ステップ 6 認証プロバイダを指定するために、**[レルム (REALM)]** のタイプを選択します。

ログインドメインを作成する前に、外部認証プロバイダを追加しておく必要があります。

ステップ 7 ログインドメインを 1 つ以上のプロバイダに割り当てます。

ドメインに割り当てる 1 つ以上のプロバイダ名の横のチェックボックスをオンにします。

次のタスク

ドメインを作成した後、[ログインドメインの編集、削除、または非アクティブ化 \(130 ページ\)](#) で説明されているように、ドメインの編集、非アクティブ化または削除を行えます。

ログインドメインの編集、削除、または非アクティブ化

1 つ以上のログインドメインを作成した後、このセクションで説明されている手順を使用して、それらを編集、削除、または非アクティブ化することができます。ローカルドメインを削除することはできませんが、非アクティブにすることはできます。

始める前に

[ログインドメインの作成 \(129 ページ\)](#) の説明に従って、1 つ以上のログインドメインを作成しておく必要があります。

ステップ 1 Cisco ACI マルチサイト 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)] > [ログインドメイン(Login Domains)]** を選択します。

ステップ 3 編集するログインドメインの横にある ... メニューをクリックします。

ドメイン情報を編集し、使用できないようにドメインを非アクティブ化するか、デフォルトとして設定して、GUI を使用してログインするときに自動的に選択されるように選択できます。

リモートユーザのログイン

外部認証が Cisco ACI マルチサイトで有効になっている場合には、以下の方法でマルチサイト Orchestrator にログインできます。

-
- ステップ1 ブラウザを使用して、マルチサイト URL に移動します。
 - ステップ2 ドロップダウン リストから、自分が割り当てられているドメインを選択します。
 - ステップ3 ユーザ名とパスワードを入力します。
 - ステップ4 [送信 (Submit)] をクリックします。
許可を受けており、認証が成功すれば、マルチサイト Orchestrator GUI が表示され、割り当てられているロールに従って権限が与えられます。パスワードは、初回ログオン時に変更する必要があります。
-

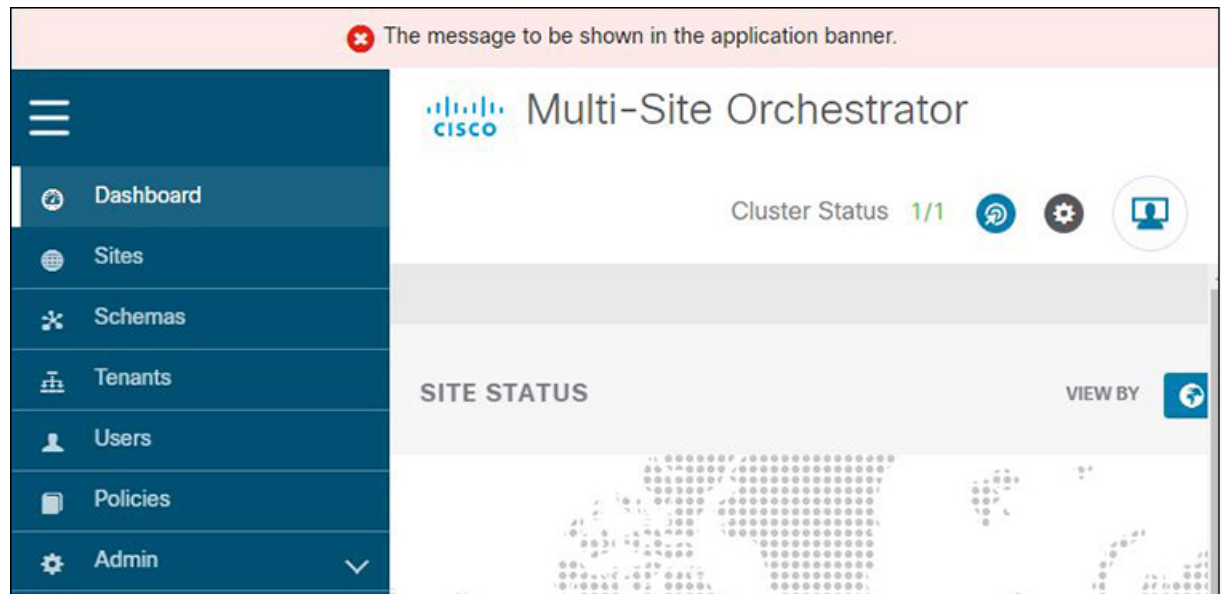
システム設定

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、マルチサイト 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 22: 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。
-

プロキシサーバ

オンプレミスとクラウドサイトの組み合わせや、社内ネットワーク内で実行されている Orchestrator などの特定の導入シナリオでは、Orchestrator はプロキシを介してインターネットおよびクラウドサイトにアクセスする必要があります。プロキシは、このセクションで説明されている方法で設定して有効にすることができます。

プロキシサーバが有効になっている場合でも、Orchestrator は、プロキシをバイパスして直接通信する、IP アドレスとホスト名の「プロキシなし」リストを維持します。このリストは、ユーザ指定のホストまたはドメインと、現在 Orchestrator に追加されているすべてのオンプレミス APIC サイトの組み合わせです。新しいサイトを Orchestrator に追加するなど、新しいアドレスでリストが更新されるたびに、プロキシサービスは再起動されます。すべてのオンプレミスサイトの完全なリストを事前に指定しておけば、サービスの再起動を最小限に抑えることができます。たとえば、プロキシ設定の構成時に、ドメイン全体を「プロキシなし」リストに追加します。

-
- 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** [プロキシサーバ (Proxy Server)] エリアの右側の [編集 (Edit)] アイコンをクリックします。
- これにより、[プロキシ設定 (Proxy Settings)] ウィンドウが開きます。
- ステップ 4** [有効化 (Enable)] を選択して、プロキシを有効にします。
- ステップ 5** [プロキシサーバ (Proxy Server)] フィールドで、プロキシサーバの IP アドレスまたはホスト名を指定します。

ステップ6 [プロキシサーバポート (**Proxy Server Port**)] フィールドで、プロキシサーバに接続するために使用するポート番号を指定します。

ステップ7 [プロキシなしリスト (**No Proxy List**)] フィールドで、プロキシをバイパスするホストとドメインのコンマ区切りのリストを指定します。

リストを指定するときには、IP アドレスまたはホスト名を指定します。または、ワイルドカード (*) 文字を使用して、ドメイン全体を指定することもできます。IP アドレスにワイルドカードを使用することはできません。

たとえば、203.0.113.1, apic1.example.com, *.example.local のようにします。

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。

プロキシを設定して有効にすると、Orchestrator アプリケーションが再起動します。



第 8 章

Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理

- Cisco Cloud APIC と Cisco ACI マルチサイトについて (135 ページ)
- Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加 (136 ページ)
- サイト間インフラストラクチャの設定 (137 ページ)
- Cisco Cloud APIC と ISN デバイス間の接続の有効化 (138 ページ)
- 共有テナントの設定 (142 ページ)
- スキーマの作成 (144 ページ)
- アプリケーションプロファイルと EPG の設定 (144 ページ)
- ブリッジドメインの作成と VRF への関連付け (145 ページ)
- コントラクトのフィルタの作成 (146 ページ)
- コントラクトの作成 (146 ページ)
- サイトをスキーマに追加する (147 ページ)
- AWS でのインスタンスの設定 (148 ページ)
- エンドポイントセレクタの追加 (150 ページ)
- Cisco ACI Multi-Site 設定の検証 (155 ページ)

Cisco Cloud APIC と Cisco ACI マルチサイトについて

セットアップウィザードを使用して Cisco Cloud APIC を設定するときに [サイト間接続 (**Inter-Site Connectivity**)] オプションを [リージョン管理 (**Region Management**)] ページで選択した場合は、Cisco ACI マルチサイトを使用して、オンプレミスサイトやクラウドサイトなどの別のサイトを、Cisco Cloud APIC サイトとともに管理します。Cisco Cloud APIC のセットアップウィザードで、[クラウドルータ (**Cloud Routers**)] オプションだけを [リージョン管理 (**Region Management**)] ページで選択した場合は、Cisco ACI マルチサイトは必要ありません。

Cisco Cloud APIC の管理専用で使用される、いくつかの新しいページが ACI マルチサイト オークストレータに導入されています。この章のトピックでは、これらの新しい Cisco Cloud APIC 管理ページについて説明します。これらの Cisco Cloud APIC 管理ページに必要な情報を入力すると、Cisco Cloud APIC は、実質的に、Cisco ACI マルチサイトを介して管理する別のサイトになります。

Cisco Cloud APIC サイトとともにオンプレミスサイトを管理している場合は、まだ設定していなければ、これらの手順を開始する前にオンプレミスサイトを設定しておくことを推奨します。これらの手順については、次の URL にある *CISCO ACI Multi Site Orchestrator Installation And Upgrade Guide* を参照してください。 <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加

-
- ステップ 1** まだログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。
- ステップ 2** メイン メニューで **[サイト]** をクリックします。
- ステップ 3** **[サイト リスト]** ページで、**[サイトの追加 (ADD SITES)]** をクリックします。
- ステップ 4** **[接続設定]** ページで、次の操作を実行します。
- [名前 (NAME)]** フィールドに、サイト名を入力します。
たとえば、cloudsite1 です。
 - (任意) **[ラベル (LABELS)]** フィールドで、ラベルを選択するか作成します。
 - [APIC CONTROLLER URL]** フィールドに、Cloud APIC の URL を入力します。これは、Amazon Web Services によって割り当てられるパブリック IP アドレスです。これは、セットアップウィザードを使用して Cloud APIC 設定 Cisco Cloud APIC する手順の開始時にログインするために使用したのと同じパブリック IP アドレスです。
たとえば、https://192.0.2.1 です。
 - [ユーザ名 (USERNAME)]** フィールドにユーザ名を入力します。
たとえば、admin とします。admin と同じ権限を持つ任意のアカウントに登録することもできます。
 - [パスワード (PASSWORD)]** フィールドに、パスワードを入力します。
 - このフィールドが自動的に入力されていない場合は、**[APIC SITE ID]** フィールドに、一意のサイト ID を入力します。
サイト ID は、Cloud APIC サイトの固有識別子である必要があります。範囲は 1 ~ 127 です。
 - [保存 (SAVE)]** をクリックします。
- ステップ 5** Cloud APIC サイトが正しく追加されたことを確認します。
- 複数のサイトを管理している場合は、ACI マルチサイト オーケストレータ の **[サイト (Sites)]** 画面にすべてのサイトを表示する必要があります。ACI マルチサイト オーケストレータ は、サイトがオンプレミスであるか、Cloud APIC サイトであるかを自動的に検出します。
-

次のタスク

[サイト間インフラストラクチャの設定 \(137 ページ\)](#) に進みます。

サイト間インフラストラクチャの設定

ステップ 1 [サイト (Sites)] ビューで、[インフラの構築 (CONFIGURE INFRA)] 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 2 左側のペインの [サイト (SITES)] の下で、クラウドサイトをクリックします。

クラウドサイト領域のほとんどすべての情報は自動的に入力され、次のステップで説明する [BGP パスワード (BGP Password)] フィールドを除き、変更できません。

ステップ 3 オンプレミス サイトとクラウド サイト間でパスワードを設定するかどうかを決定します。

- オンプレミス サイトとクラウド サイトの間でパスワードを設定しない場合は、[ステップ 4 \(137 ページ\)](#) に進みます。
- オンプレミス サイトとクラウド サイト間でパスワードを設定するには、次のようにします。
 - a) 右側のペインで、[BGP パスワード (BGP password)] フィールドをクリックして、パスワードを入力します。
 - b) [CloudSite] ウィンドウの右上隅にある [更新 (Refresh)] アイコンをクリックします。

すべてのクラウド プロパティは、Cloud APIC から自動的に取得されます。サイトが正常に更新されたことを示すメッセージが表示され、すべてのクラウド プロパティが Cloud APIC から正常に取得されたことを確認します。

ステップ 4 クラウド サイトでマルチサイト接続を有効にするには、[ACI マルチサイト (ACI Multi-Site)] ボタンをクリックします。

ステップ 5 サイト間インフラストラクチャを設定するために使用する展開のタイプを選択します。

画面の右上にある [展開 (Deploy)] ボタンをクリックすると、次のスクロールダウンメニューオプションが表示されます。

- **[展開のみ (Deploy Only):]** マルチクラウド (クラウドサイトからクラウドサイト) への接続を設定する場合は、このオプションを選択します。

このオプションは、クラウドサイトと Cloud APIC サイトに設定をプッシュし、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接続を有効にします。
- **[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 Cloud 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接続を有効にします。さらに、このオプションでは、AWS に導入された Cisco クラウド サービスルータ 1000V (CSR) とオンプレミスの IPsec 終端 デバイスとの間の接続を有効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):]** AWS に展開された Cisco Cloud Services Router 1000V (CSR) とオンプレミスの IPsec 終端デバイス間の接続を有効にするために使用する、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。

Cisco Cloud APIC と ISN デバイス間の接続の有効化



- (注) このセクションの手順は、オンプレミス サイトとクラウド サイト間の接続を有効にしている場合にのみ実行してください。オンプレミス サイトがない場合は、これらの手順をスキップして、[共有テナントの設定 \(142 ページ\)](#) に進みます。

Amazon Web Services に展開された Cisco Cloud Services Router 1000V (CSR) とオンプレミスの IPsec ターミネーション デバイス間の接続を手動で有効にするには、次の手順に従います。

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。

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 AWS 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。

- [サイト間インフラストラクチャの設定 \(137 ページ\)](#) で示されている手順の一部として ACI マルチサイト オーケストレータで、**IPN デバイス設定ファイルを展開してダウンロードするか、IPN デバイス設定ファイルのみをダウンロードする**ように選択した場合、ISN デバイスの設定ファイルが含まれている zip ファイルを見つけます。
- AWS に展開された 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情報を手動で検索する場合は、『*Cisco Cloud APIC インストール ガイド*』の付録で説明されているように、CSR とテナントの情報を収集します。

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。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、最初の CSR の設定情報を見つけて、その設定情報を入力します。

次に、最初の CSR の設定情報がどのように表示されるかの例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-<first-CSR-tunnel-ID>
  pre-shared-key address <first-CSR-elastic-IP-address> key <first-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CSR-tunnel-ID>
  local-address <interface>
  match identity address <first-CSR-elastic-IP-address>
  keyring infra:overlay-1-<first-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CSR-tunnel-ID> esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel <first-CSR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
  tunnel destination <first-CSR-elastic-IP-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf <process-id> area <area-id>
  no shut
exit
```

ここで、

- <first-CSR-tunnel-ID> は、このトンネルに割り当てる一意のトンネル ID です。
- <first-CSR-tunnel-ID> は、最初の CSR の3番目のネットワーク インターフェイスの柔軟な IP アドレスです。
- <first-CSR-preshared-key> は、最初の CSR の事前共有キーです。
- <interface> は、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。

- <peer-tunnel-for-onprem-IPsec-to-first-CSR> は、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> は OSPF プロセス ID です。
- <area-id> は、OSPF エリア ID です。

次に例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-1000
  pre-shared-key address 192.0.2.20 key 123456789009876543211234567890
exit

crypto isakmp profile infra:overlay-1-1000
  local-address GigabitEthernet1
  match identity address 192.0.2.20
  keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1000
  ip address 30.29.1.2 255.255.255.252
  ip virtual-reassembly
  tunnel source GigabitEthernet1
  tunnel destination 192.0.2.20
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-1000
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf 1 area 1
  no shut
exit
```

ステップ 4 2 番目の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、2 番目の CSR の設定情報を見つけて、その設定情報を入力します。

次に、2 番目の CSR の設定情報がどのように見えるかの例を示します。

```
crypto isakmp policy 1
  encryption aes
```



```
    authentication pre-share
    group 2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<second-CSR-tunnel-ID>
    pre-shared-key address <second-CSR-elastic-IP-address> key <second-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<second-CSR-tunnel-ID>
    local-address <interface>
    match identity address <second-CSR-elastic-IP-address>
    keyring infra:overlay-1-<second-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <second-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-second-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <second-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

次に例を示します。

```
crypto isakmp policy 1
    encryption aes
    authentication pre-share
    group 2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1001
    pre-shared-key address 192.0.2.21 key 123456789009876543211234567891
exit

crypto isakmp profile infra:overlay-1-1001
    local-address GigabitEthernet1
    match identity address 192.0.2.21
    keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
    mode tunnel
exit
```

```

crypto ipsec profile infra:overlay-1-1001
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1001
  ip address 30.29.1.6 255.255.255.252
  ip virtual-reassembly
  tunnel source GigabitEthernet1
  tunnel destination 192.0.2.21
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-1001
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf 1 area 1
  no shut
exit

```

ステップ 5 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 6 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。

次に例を示します。

```

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

```

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。

共有テナントの設定

オンプレミスサイトと Cloud APIC サイト間で共有されるテナントを設定するには、この項の手順に従います。

ステップ 1 ACI マルチサイト オーケストレータで、次の手順を実行します。

- a) メインメニューで、[テナント (Tenants)] をクリックします。
- b) [テナントリスト (Tenants List)] エリアで、[テナントの追加 (ADD TENANT)] をクリックします。
- c) [テナントの詳細 (Tenant Details)] ペインで、次の手順を実行します。
 - [表示名 (DISPLAY NAME)] フィールドに、テナント名を入力します。
 - オプション: [説明 (DESCRIPTION)] フィールドに、テナントについての簡潔な説明を入力します。
 - [関連するサイト (Associated Sites)] セクションで、オンプレミスとクラウドのサイトを選択します。

- まだ選択していなければ、**[関連するユーザ (Associated Users)]** セクションで、ユーザを選択します。
- **[保存 (SAVE)]** をクリックします。

ステップ 2 Cloud APICサイトにログインし、このテナントの Amazon Web Services アカウントの詳細を設定します。

- a) メインの Cloud APIC ページの **[アプリケーション管理 (Application Management)]** の下で、**[テナント (Tenant)]** をクリックします。
- b) **[テナント (Tenant)]** ページで、前の手順の ACI マルチサイト オーケストレータ で作成したテナントをクリックします。
- c) 画面の右上にある展開ボタンをクリックします。
これは、**[閉じる (X)]** ボタンの横にある、正方形と上向きの矢印が付いたボタンです。
- d) **[テナント (Tenant)]** ページで、画面の右上にある編集ボタンをクリックします。これは、**[アクション (Actions)]** フィールドの横にある、鉛筆のアイコンが付いたボタンです。
- e) **[テナントの編集 (Edit Tenant)]** ページで、**[設定 (Settings)]** 領域までスクロールし、Cloud APIC のユーザテナントが信頼できるかどうかに応じて必要な情報を入力します。

- Cloud APIC のユーザテナントが信頼されている場合 (CFT を使用して信頼できるテナントの AWS アカウントを設定した場合) は、このページに次の情報を入力します。

- **[信頼できるテナント (Trusted Tenant):]** このボックスは、デフォルトでオンになっているはずです。そうになっていなかった場合には、チェックボックスをオンにして、この機能を有効にします。

- **[クラウドアカウント ID (Cloud Account ID):]** ユーザテナントの AWS アカウント番号 (CFT を使用して、信頼できるテナントの AWS アカウントをセットアップしたときにログインした AWS アカウント) を入力します。

(注) **[クラウドアクセス キー ID (Cloud Access KEY ID)]** フィールドと **[クラウド秘密アクセス キー (Cloud Secret Access Key)]** フィールドは、**[信頼済みテナント (Trusted Tenant)]** ボックスをオンにしても表示されません。これらのフィールドは、信頼できるテナントには必要ありません。

- Cloud APICのユーザテナントが信頼されていない場合 (AWS アクセスキー ID と秘密アクセスキーを使用して、信頼できないユーザテナントの AWS アカウントをセットアップした場合) は、このページで次の情報を入力します。

- **[信頼できるテナント (Trusted Tenant):]** この機能を無効にするには、このチェックボックスをオフにします。

- **[クラウドアカウント ID (Cloud Account ID):]** このフィールドには、ユーザテナントの AWS アカウント番号を入力します。

- **[クラウドアクセス キー ID (Cloud Access KEY ID):]** このフィールドには、ユーザテナントの AWS アクセスキー ID 情報を入力します。

- **[クラウド秘密アクセス キー (Cloud Secret Access Key):]** このフィールドには、ユーザ テナントの AWS 秘密アクセス キー情報を入力します。

f) 画面の下部にある**[保存 (Save)]** をクリックします。

次のタスク

[スキーマの作成 \(144 ページ\)](#) に進みます。

スキーマの作成

Cisco Cloud APIC に固有ではない一般的な Cisco ACI Multi-Site 手順がいくつかありますが、Cisco ACI Multi-Site を介してオンプレミスサイトと Cisco Cloud APIC サイトを管理している場合は Cisco Cloud APIC の全体的なセットアップの一部として実行する必要があります。ここでは、APIC の Cisco Cloud 全体的なセットアップの一部である Cisco ACI Multi-Site の一般的な手順について説明します。

Cisco Cloud APIC サイトの新しいスキーマを作成する場合は、この項の手順に従ってください。

Cisco Cloud APIC サイトに使用するスキーマがすでにある場合は、これらの手順をスキップして、[サイトをスキーマに追加する \(147 ページ\)](#) に移動することができます。

-
- ステップ 1** メイン メニューで **[スキーマ]** をクリックします。
 - ステップ 2** **[スキーマ]** ページで、**[スキーマの追加]** をクリックします。
 - ステップ 3** **[無題スキーマ]** ページで、ページの上部にあるテキスト **無題スキーマ** を、作成するスキーマの名前 (たとえば、**Cloudbursting スキーマ**) に置き換えます。
 - ステップ 4** 左側のペインで **[ロール (Roles)]** をクリックします。
 - ステップ 5** 中央のペインで、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をクリックしてください。
 - ステップ 6** **[テナントの選択]** ダイアログ ボックスにアクセスし、ドロップダウン メニューから **共有テナントの設定 (142 ページ)** で作成したテナントを選択します。
-

アプリケーション プロファイルと EPG の設定

この手順では、アプリケーション プロファイルを設定し、2つの EPG を追加する方法について説明します。1つはクラウドサイト用、もう1つは、プロバイダ コントラクトが1つの EPG に関連付けられており、コンシューマ コントラクトが他の EPG に関連付けられている場合です。

- ステップ 1 中央のペインで、[アプリケーションプロファイル (Application Profile)] エリアを見つけて、[+ アプリケーションプロファイル (+ Application profile)] をクリックします。
- ステップ 2 右側のペインで、[表示名 (DISPLAY NAME)] フィールドにアプリケーションプロファイルの名前を入力します。
- ステップ 3 中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックして、クラウドサイトの EPG を作成します。
- ステップ 4 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば ep1)。
- ステップ 5 オンプレミスサイトの EPG を作成する場合には、中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックします。
- ステップ 6 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば ep2)。
- ステップ 7 VRF を作成します。
 - a) 中央のペインで、[VRF] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
 - b) 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば vrf1)。
- ステップ 8 [保存 (SAVE)] をクリックします。

ブリッジドメインの作成と VRF への関連付け

この項の手順に従って、オンプレミスサイトのブリッジドメインを作成し、それを VRF に関連付けます。これらの手順は、クラウドのみのスキーマには必要ではないことに注意してください。

- ステップ 1 中央のペインで、[EPG] まで上にスクロールして戻り、以前にオンプレミスサイト用に作成した EPG をクリックします。
- ステップ 2 右側のペインの[オンプレミスプロパティ (ON-PREM PROPERTIES)] エリアの[ブリッジドメイン (BRIDGE DOMAIN)] の下で、フィールドに名前を入力し (たとえば、bd1)、[作成 (create)] エリアをクリックして新しいブリッジドメインを作成します。
- ステップ 3 中央のペインで、今作成したブリッジドメインをクリックします。
- ステップ 4 [仮想ルーティング/フォワーディング (Virtual Routing & Forwarding)] フィールドで、[アプリケーションプロファイルと EPG の設定 \(144 ページ\)](#) で作成した VRF を選択します。
- ステップ 5 [サブネット (SUBNETS)] エリアまで下にスクロールし、[GATEWAY (ゲートウェイ)] 見出しの下の [サブネット (SUBNET)] の横にある + をクリックします。
- ステップ 6 [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、追加する予定のサブネットの説明を入力します。このゲートウェイ IP アドレスは、オンプレミスのサブネットのもので、
- ステップ 7 [範囲 (Scope)] フィールドで、[外部にアドバタイズ (Advertised Externally)] を選択します。

ステップ 8 [保存 (SAVE)] をクリックします。

コントラクトのフィルタの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、[表示名 (DISPLAY NAME)] フィールドにフィルタの名前を入力します。

ステップ 3 [+ 入力 (+ Entry)] をクリックして、[エントリの追加 (Add Entry)] ディスプレイ上のスキーマフィルタについての情報を入力します。

- Name** フィールド (Add Entry ダイアログ) のスキーマ フィルタ エントリの名前を入力します。
- オプション。 **Description** フィールドにフィルタの説明を入力します。
- EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

TYPE: IP、IP PROTOCOL: TCP、および DESTINATION PORT RANGE FROM および DESTINATION PORT range TO: https。

- [保存 (SAVE)] をクリックします。
-

コントラクトの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、[表示名 (DISPLAY name)] フィールドにコントラクトの名前を入力します。

ステップ 3 [範囲 (SCOPE)] エリアで、VRF の選択をそのままにします。

ステップ 4 [フィルタ チェーン (FILTER CHAIN)] エリアで、[+ フィルタ (+ FILTER)] をクリックします。

[フィルタ チェーンの追加 (Add Filter Chain)] 画面が表示されます。

ステップ 5 [名前 (NAME)] フィールドで、[コントラクトのフィルタの作成 \(146 ページ\)](#) で作成したフィルタを選択します。

ステップ 6 中央のペインで、[EPG] までスクロールして戻り、クラウド サイト用に作成した EPG をクリックします。

ステップ 7 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。

[コントラクトの追加] 画面が表示されます。

- ステップ 8 [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 9 [タイプ (TYPE)] フィールドで、コンシューマまたはプロバイダのいずれかを選択します。
- ステップ 10 [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、アプリケーションプロファイルと EPG の設定 (144 ページ) で作成した VRF を選択します。
- ステップ 11 [保存 (SAVE)] をクリックします。
- ステップ 12 中央のペインで、[EPG] までスクロールして戻り、オンプレミスサイト用に作成した EPG をクリックします。
- ステップ 13 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。
[コントラクトの追加] 画面が表示されます。
- ステップ 14 [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 15 [タイプ (TYPE)] フィールドで、[コンシューマ (CONSUMER)] または [プロバイダ (PROVIDER)] を選択します。これは、前の EPG に選択しなかったものです
たとえば、最初の EPG に [プロバイダ (PROVIDER)] を選択した場合は、2 番目の EPG の [コンシューマ (CONSUMER)] を選択します。
- ステップ 16 [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、アプリケーションプロファイルと EPG の設定 (144 ページ) で作成したのと同じ VRF を選択します。

サイトをスキーマに追加する

- ステップ 1 左側のペインで、[サイト (Sites)] の横にある + をクリックします。
- ステップ 2 [サイトの追加 (Add Sites)] ページで、それぞれの横にあるボックスをオンにして、オンプレミスおよびクラウドサイトをスキーマに追加し、[保存 (Save)] をクリックします。
- ステップ 3 左側のペインのクラウドサイトの下にあるテンプレートをクリックして、テンプレートのサイトローカルプロパティを設定します。
- ステップ 4 中央のペインで、VRF をクリックします。
- ステップ 5 右側のペインの [サイトローカル プロパティ (SITE LOCAL PROPERITES)] 領域で、次の情報を入力します。
- [リージョン (region)] フィールドで、この VRF を導入する Amazon Web サービスのリージョンを選択します。
 - CIDR フィールドで、+CIDR をクリックします。
- [クラウド CIDR の追加 (ADD CLOUD CIDR)] ダイアログボックスが表示されます。次の情報を入力します。
- CIDR: VPC CIDR 情報を入力します。たとえば、11.11.0.0/16 とします。

CIDR には、Amazon Web Services VPC で使用可能になるすべてのサブネットの範囲が含まれています。

(注) このフィールドに入力した VPC CIDR 情報は、インフラ VPC CIDR と重複させることはできません。このフィールドに入力した CIDR 情報が、AWS で Cloud APIC を導入するの 12 の [インフラ VPC プール (Infra VPC Pool)] フィールドに入力したインフラ VPC CIDR 情報と重複していないことを確認します。

- **[CIDR タイプ (CIDR TYPE)]:** [プライマリ (Primary)] または [セカンダリ (Secondary)] を選択します。これが最初の CIDR の場合は、CIDR タイプとして [プライマリ (Primary)] を選択します。
- **[サブネット追加 (ADD SUBNETS)]:** サブネット情報を入力し、ゾーンを選択してから、チェックマークをクリックします。たとえば、11.11.1.0/24 とします。

サブネットは、各アベイラビリティゾーンの CIDR ブロックの範囲内に割り当てます。

c) ウィンドウで [保存 (Save)] をクリックします。

AWS でのインスタンスの設定

Cloud APIC のためのエンドポイントセレクトアを、Cloud APIC GUI または ACI マルチサイトオーケストレータ GUI のいずれかを使用して設定する場合には、Cloud APIC のために設定するエンドポイントセレクトアに対応し、AWS 内で必要なインスタンスについても、設定する必要があります。

このトピックでは、AWS でインスタンスを設定する手順について説明します。Cloud APIC のためのエンドポイントセレクトアを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを設定することができます。たとえば、先に AWS のアカウントに移動し、AWS のカスタムタグまたはラベルを作成してから、ACI マルチサイトオーケストレータのカスタムタグまたはラベルを使用して、エンドポイントセレクトアを作成することができます。または、ACI マルチサイトオーケストレータでカスタムタグまたはラベルを使用してエンドポイントセレクトアを作成してから、AWS のアカウントに移動し、AWS のカスタムタグまたはラベルを作成することもできます。

ステップ 1 ACI マルチサイトオーケストレータ GUI または Cisco Cloud APIC GUI を使用してクラウドコンテキストプロファイルを設定したかどうかを確認します。

クラウドコンテキストプロファイルは、AWS インスタンス設定プロセスの一部として設定する必要があります。ここで、クラウドコンテキストプロファイルは、VRF およびリージョンと組なって、そのリージョン内の AWS VPC を表します。Cisco Cloud APIC GUI を使用してクラウドコンテキストプロファイルを設定すると、VRF やリージョンの設定などの設定情報は、AWS にプッシュされます。同様のアクションは、Cisco Cloud APIC を ACI マルチサイトオーケストレータ GUI を使用して設定した場合にも生じます。ここで、これらのクラウドコンテキストプロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として ACI マルチサイトオーケストレータ GUI によって設定され、AWS にプッシュされます。

- Cisco Cloud APIC を ACI マルチサイト オーケストレータ GUI を使用して設定する場合は、クラウド コンテキスト プロファイルを手動で設定する必要はありません。VRF やリージョン設定など、特定のクラウド コンテキスト プロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として、前のセクションで実行した ACI マルチサイト オーケストレータ GUI により設定され、AWS にプッシュされます。
- クラウド コンテキスト プロファイルを Cisco Cloud APIC GUI を使用して設定する場合には、『Cisco Cloud APIC User Guide, Release 4.1(x)』で説明されている手順に従い、GUI または REST API を使用して、クラウド コンテキスト プロファイルを設定してください。

- ステップ 2** クラウド コンテキスト プロファイルの設定を確認し、AWS インスタンスで使用する設定を決定します。
- a) まだログインしていない場合は、Cisco Cloud APIC にログインします。
 - b) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。
 - c) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。
Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。
 - d) この AWS インスタンス設定プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウド コンテキスト プロファイルのさまざまな設定パラメータが表示されます。AWS インスタンスを設定するときには、このウィンドウに表示される情報を使用します。
- ステップ 3** まだログインしていない場合は、Cisco Cloud APIC ユーザテナントの Amazon Web Services アカウントにログインします。
- ステップ 4** **[サービス (Services)] > EC2 > インスタンス (Instances) > [インスタンスの起動 (Launch Instance)]** に移動します。
- ステップ 5** **[Amazon マシン イメージ (AMI) の選択 (Choose Amazon Machine Image (AMI))]** ページで、Amazon マシン イメージ (AMI) を選択します。
- ステップ 6** **[インスタンス タイプの選択 (Choose An Instance type)]** ページで、インスタンス タイプを選択し、**[インスタンスの詳細の設定 (Configure instance Detail)]** をクリックします。
- ステップ 7** **[インスタンスの詳細の設定 (Configure instance Detail)]** ページで、該当するフィールドに必要な情報を入力します。
- **[ネットワーク (Network)]** フィールドで、Cloud APIC VRF を選択します。
これは、この AWS インスタンス設定プロセスの一部として使用しているクラウド コンテキスト プロファイルに関連付けられている VRF です。
 - **[サブネット (Subnet)]** フィールドに、サブネットを入力します。
 - パブリック IP を使用する場合は、**[パブリック IP の自動割り当て (Auto Assign public IP)]** フィールドで、スクロールダウンメニューから **[有効 (Enable)]** を選択します。

- ステップ 8** [インスタンスの詳細の設定 (Configure Instance Details)] ページに必要な情報を入力したら、[ストレージを追加 (Add Storage)] をクリックします。
- ステップ 9** [ストレージの追加 (Add Storage)] ページで、デフォルト値を受け入れるか、必要に応じてこのページでストレージを設定し、[タグの追加 (add Tags)] をクリックします。
- ステップ 10** [タグの追加 (Add Tags)] ページで、[タグの追加 (add Tag)] をクリックし、このページの該当するフィールドに必要な情報を入力します。

(注) これらの手順の後の部分で、エンドポイントセレクタのタイプに対して IP アドレス、リージョン、またはゾーンを使用する場合は、このページに情報を入力する必要はありません。このような状況では、AWS でインスタンスを開始すると、Cloud APIC によって IP アドレス、リージョン、またはゾーンが検出され、エンドポイントが EPG に割り当てられます。

- **[キー (Key):]** これらの手順で後で追加するエンドポイントセレクタのタイプのカスタム タグを作成するときに使用するキーを入力します。
- **[値 (Value):]** このキーで使用する値を入力します。
- **[インスタンス (Instance):]** このフィールドのチェックボックスをオンにします。
- **[ボリューム (Volume):]** このフィールドのチェックボックスをオンにします。

たとえば、これらの手順で後ほど、エンドポイントセレクタの特定のビルディングのカスタムタグを作成する予定の場合 (building6 など) は、このページの次のフィールドに次の値を入力できます。

- **[キー (Key):]** ロケーション
- **[値 (value):]** building6

- ステップ 11** [確認して起動する (Review and Launch)] をクリックします。

既存のキー ペアを選択するか、新しいキー ペアを作成します。キーペアの ページが表示されます。後ほどインスタンスに ssh 接続する場合は、このページの情報を使用します。

エンドポイントセレクタの追加

Cisco Cloud APIC では、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウド EPG に割り当てるために使用される、エンドポイントセレクタと呼ばれる機能があります。エンドポイントセレクタは、基本的に言って、Cisco ACI によって管理される AWS VPC に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイント インスタンスに一致するエンドポイントセレクタルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイントセレクタは、Cisco ACI で使用可能な属性ベースのマイクロセグメンテーションに似ています。

エンドポイントセレクタは、Cisco Cloud APIC GUI または ACI マルチサイト オーケストレータ GUI のいずれかを使用して設定できます。2つの GUI 間で使用可能なオプションにはわずかな違いがありますが、エンドポイントセレクタを追加するための一般的な概念と全体的な手順は、基本的にこの2つの間で同じです。

このセクションの手順では、ACI マルチサイト オーケストレータ GUI を使用してエンドポイントセレクタを設定する方法について説明します。Cisco Cloud APIC GUI を使用したエンドポイントセレクタの設定の詳細については、『Cisco Cloud APIC User Guide, Release 4.1 (x)』を参照してください。

ステップ 1 Cisco Cloud APIC のエンドポイントセレクタに使用できる Amazon Web Services サイトから、必要な情報を収集します。

手順については、[AWS でのインスタンスの設定 \(148 ページ\)](#) を参照してください。

(注) これらの手順は、最初に AWS でインスタンスを設定してから、その後に Cisco Cloud APIC のエンドポイントセレクタを追加することを前提としています。ただし、[AWS でのインスタンスの設定 \(148 ページ\)](#) で説明されているように、最初に Cisco Cloud APIC のエンドポイントセレクタを追加してから、この AWS インスタンスの設定手順を、これらのエンドポイントセレクタの手順の最後で実行することもできます。

ステップ 2 ログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。

ステップ 3 左側のペインで、**[スキーマ (schema)]** をクリックし、以前に作成したスキーマを選択します。

ステップ 4 エンドポイントセレクタを作成する方法を決定します。

- 今後追加される、任意のクラウドサイトに適用できるエンドポイントセレクタを作成するには、次の手順を実行します。
 1. 左側のペインで、テンプレートを選択したままにします。
これらの手順で特定のサイトを選択しないでください。
 2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。
 3. 右側のペインの **[クラウドのプロパティ (CLOUD PROPERTIES)]** 領域で、**+[セレクタ (SELECTORS)]** の横にあるものをクリックして、エンドポイントセレクタを設定します。
 4. **[新しいエンドポイントセレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイントセレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイントセレクタで使用する分類に基づいて名前を入力します。
 5. **[+ 式 (Expression)]** をクリックし、エンドポイントセレクタのタイプを選択します。
このように作成されたエンドポイントセレクタの場合、**[キー (Key)]** フィールドで使用できるオプションは **[EPG]** のみです。
 6. [ステップ 5 \(152 ページ\)](#) に進みます。
- このクラウドサイト専用のエンドポイントセレクタを作成するには、次の手順を実行します。

1. 左ペインで、クラウドサイトを選択します。
2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。
3. 右側のペインの **[サイトのローカルのプロパティ (SITE LOCAL PROPERITES)]** 領域の **[セレクタ (SELECTOR)]** 領域で、+ **([セレクタ (SELECTOR)]** の横にあるもの) をクリックして、エンドポイントセレクタを設定します。
4. **[新しいエンドポイントセレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイントセレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイントセレクタで使用する分類に基づいて名前を入力します。

たとえば、IPサブネット分類のエンドポイントセレクタの場合は、`[IP-Subnet-EPSelector]` などの名前を使用できます。

5. **[+ 式 (Expression)]** をクリックし、エンドポイントセレクタで使用するキーを選択します。
 - **[IP アドレス (IP Address)]**: IP アドレスまたはサブネットによって選択するために使用されます。
 - **[リージョン (Region)]**: エンドポイントの AWS リージョンで選択するために使用されます。
 - **[ゾーン (Zone)]**: エンドポイントの AWS アベイラビリティゾーンによって選択するために使用されます。
 - エンドポイントセレクタのカスタムタグを作成する場合は、**[検索または作成のために入力 (Type to search or create)]** フィールドで入力を開始してカスタムタグまたはラベルを入力し、新しいフィールドで **[作成 (Create)]** をクリックして、新しいカスタムタグまたはラベルを作成します。

AWS にタグを追加するときに、これらの手順の前の例を使用すると、以前に AWS で追加したロケーションタグと一致するように、このフィールドにカスタムタグのロケーションを作成できます。

ステップ 5 **[演算子 (Operator)]** フィールドで、エンドポイントセレクタに使用する演算子を選択します。

- (注) 4.2(1) より前のリリースでは、オプションとして **[キーが存在 (Key Exist)]** と **[キーが存在しない (Key Not Exist)]** を使用していましたが、現在では **[キーを持つ (Has Key)]** と **[キーを持たない (Does Not Have Key)]** になっています。異なるのはオプションの名前だけで、機能はどちらのオプションのセットでも同じです。

次のオプションがあります。

- **[等しい (Equals)]**: [値 (value)] フィールドに 1 つの値がある場合に使用します。
- **[等しくない (Not Equals)]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある (In)]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない (Not In)]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ (Has Key)]**: 式にキーのみが含まれている場合に使用されます。

- [キーを持たない (Does Not Have Key)]: 式にキーのみが含まれている場合に使用されます。

ステップ 6 [値 (value)] フィールドで、2つ前のフィールドに対して行った選択に基づいて、エンドポイントセレクタに使用する値を選択します。[値 (Value)] フィールドには、複数のカンマ区切りのエントリを含めることができます。このフィールドのエントリの間には論理 OR があるものとみなされます。

(注) [キーを持つ (Has Key)] または [キーを持たない (Does Not Have Key)] を選択していない場合には、[演算子 (Operator)] フィールドは表示されません。

たとえば、エンドポイントセレクタに、us-west-1a など特定の Amazon Web サービスのアベイラビリティゾーンを設定する場合には、この画面で次の項目を選択します。

- [キー (Key):] Zone
- [演算子 (Operator):] Equals
- [値 (Value):] us-west-1a

別の例として、これらのフィールドで次の値を使用したとします。

- [キー (Key):] IP
- [演算子 (Operator):] Has Key
- [値 (Value):] は、演算子 (Operator) フィールドで [Has Key] が使用されているため、使用できません。

EPG ルールは、この状況で IP アドレスを持つすべてのエンドポイントに適用されます。

最後の例として、これらのフィールドで次の値を使用したとします。

- [キー (Key):] custom tag: Location
- [演算子 (Operator):] Has Key
- [値 (Value):] は、演算子 (Operator) フィールドで [Has Key] が使用されているため、使用できません。

この場合、EPG ルールは、AWS タグキーとして Location を持つすべてのエンドポイントに、ロケーションの値に関係なく適用されます。

ステップ 7 このエンドポイントセレクタ式の作成が完了したら、チェックマークをクリックします。

ステップ 8 追加のエンドポイントセレクタ式を作成するかどうかを決定します。

単一のエンドポイントセレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイントセレクタ 1、式 1:
 - [キー (Key):] Zone
 - [演算子 (Operator):] Equals
 - [値 (Value):] us-west-1a

- エンドポイントセクタ1、式2:
 - [キー (Key):] IP
 - [演算子 (Operator):] Equals
 - [値 (Value):] 192.0.2.1/24

この場合、これらの式の両方が真になる場合 (アベイラビリティゾーンが `us-west-1a` で、IP アドレスがサブネット `192.0.2.1/24` に属している場合) に、そのエンドポイントはクラウド EPG に割り当てられます。

このエンドポイントセクタで作成するすべての式を追加した後で、チェックマークをクリックします。

ステップ 9 このエンドポイントセクタの式の作成が完了したら、**[保存 (SAVE)]** をクリックします。これは **[新しいエンドポイントセクタの追加 (Add New End Point selector)]** の右下隅にあります。

EPG の下で複数のエンドポイントセクタを作成した場合は、それらのエンドポイントセクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイントセクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイントセクタを作成したとします。

- エンドポイントセクタ 2、式1:
 - [キー (Key):] Region
 - [演算子 (Operator):] In
 - [値 (Value):] `us-east-1a`, `us-east-2`

その場合、次のようになります。

- アベイラビリティゾーンが `us-west-1a` で、IP アドレスが `192.0.2.1/24` サブネットに属している (エンドポイントセクタ 1 の式)
- または
- リージョンが `us-east-1a` または `us-east-2` (エンドポイントセクタ 2 の式) のいずれかである

その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 10 エンドポイントセクタの作成が完了したら、右上隅の **[保存 (SAVE)]** をクリックします。

ステップ 11 画面の右上隅にある **[サイトに展開 (DEPLOY TO SITES)]** ボタンをクリックして、スキーマをサイトに展開します。

[正常に展開 (Successfully Deployed)] されたというメッセージが表示されます。

次のタスク

[Cisco ACI Multi-Site 設定の検証 \(155 ページ\)](#) の手順を使用して、Cisco ACI マルチサイトエリアが正しく設定されていることを確認します。

Cisco ACI Multi-Site 設定の検証

このトピックの手順を使用して、ACI マルチサイト オーケストレータ に入力した設定が正しく適用されていることを確認します。

ステップ 1 Cloud APIC にログインし、次のことを確認します。

- a) [ダッシュボード (Dashboard)] をクリックし、オンプレミス接続ステータスおよびリージョン間接続ステータスボックスの情報を使用して、次のことを確認します。
 - トンネルは、AWS 上の Cisco Cloud Services Router 1000V から、オンプレミスの ISN (IPsec ターミネーションポイント)、およびユーザ VPC の VGW に対して動作しています。
 - OSPF ネイバーが Cisco Cloud サービス ルータと ISN オンプレミス デバイスの間で起動していることを示します。
 - VRF の BGP EVPN ルートにはクラウドとオンプレミスのルートが表示され、クラウドルートは ACI スパイン スイッチの BGP EVPN を介して入力されます。
- b) [アプリケーション管理 (Application Management)] → [テナント] をクリックし、テナントが正しく設定されていることを確認します。
- c) [アプリケーション管理 (Application Management)] → [アプリケーションプロファイル] をクリックし、アプリケーションプロファイルが正しく設定されていることを確認します。
- d) [アプリケーション管理 (Application Management)] → [EPG] をクリックし、EPG が正しく設定されていることを確認します。
- e) [アプリケーション管理 (Application Management)] → [コントラクト] をクリックし、契約が正しく設定されていることを確認します。
- f) [アプリケーション管理 (Application Management)] → [VRF] をクリックし、VRF が正しく設定されていることを確認します。
- g) [アプリケーション管理 (Application Management)] → [クラウド コンテキスト Cloudプロファイル] をクリックし、クラウド コンテキストプロファイルが正しく設定されていることを確認します。
- h) [クラウドリソース (Cloud Resources)] → [リージョン] をクリックし、リージョンが正しく設定されていることを確認します。
- i) [クラウドリソース (Cloud Resources)] → [VPC] をクリックし、VPC が正しく設定されていることを確認します。
- j) [クラウドリソース (Cloud Resources)] → [クラウドエンドポイント] をクリックし、クラウドエンドポイントが正しく設定されていることを確認します。
- k) [クラウドリソース (Cloud Resources)] → [ルータ] をクリックし、CSR が正しく設定されていることを確認します。

ステップ 2 オンプレミスの APIC サイトにログインし、APIC のスキーマを確認します。

ACI マルチサイト オーケストレータ で設定した共有テナントが APIC のテナントエリアに表示され、ACI マルチサイト オーケストレータ スキーマから展開された VRF と EPG がオンプレミス APIC で設定されていることが確認できます。

ステップ3 コマンドラインから、AWS の Cisco Cloud サービス ルータ 1000V で VRF が正しく作成されていることを確認します。

```
show vrf
```

テナントt1と VRF v1が ACI マルチサイト オーケストレータ から展開されている場合、CSR の出力は次のようになります。

Name	Default RD	Protocols	Interfaces
t1:v1	64514:3080192	ipv4	BD1 Tu4 Tu5

ステップ4 コマンドラインから、AWS サービス ルータ 1000V と ISN オンプレミス デバイスの間 Cisco Cloud でトンネルがアップしていることを確認します。

AWS または ISN オンプレミスのデバイスで、Cisco Cloud サービス ルータ 1000V で次のコマンドを実行できます。

```
show ip interface brief | inc Tunnel
```

以下のような出力が表示されます。

Interface	IP-Address	OK?	Method	Status	Protocol
Tunnel1	1.2.3.22	YES	manual	up	up
Tunnel2	1.2.3.30	YES	manual	up	up
Tunnel3	1.2.3.6	YES	manual	up	up
Tunnel4	1.2.3.14	YES	manual	up	up

ステップ5 コマンドラインから、OSPF ネイバーが AWS 上の Cisco Cloud サービス ルータ 1000V と ISN オンプレミス デバイスの間でアップしていることを確認します。

```
show ip ospf neighbor
```

以下のような出力が表示されます。

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.200.10.201	0	FULL/ -	00:00:36	1.2.3.13	Tunnel4
20.30.40.50	0	FULL/ -	00:00:36	1.2.3.29	Tunnel2
10.202.101.202	0	FULL/ -	00:00:38	1.2.3.5	Tunnel3

ステップ6 コマンドラインから、オンプレミスの BGP EVPN ネイバーが Cisco Cloud サービス ルータ 1000V に存在することを確認します。

```
show bgp l2vpn evpn summary
```

以下のような出力が表示されます。

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.2	4	100	139	137	99	0	0	01:30:36	6

ステップ7 コマンドラインから、VRF の BGP ルートにクラウドとオンプレミスの両方のルートが表示されていることを確認します。

(注) 現在 Cloud APIC のワークフローでは、VRF は、対応する VPC が AWS で作成されるまで、Cisco Cloud サービスルータ 1000V で設定されません。

```
show ip route vrf t1:v1
```

以下のような出力が表示されます。

```
B    129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1  
B    130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```
