L3Out のノードとインターフェイス

- L3Out のインターフェイスの変更 （1 ページ）
- OSPF インターフェイス プロファイルの作成 （3 ページ）
- OSPF タイマー ポリシーを作成 （8 ページ）
- OSPF 最大メトリック （12 ページ）
- L3Out の SVI のカスタマイズ （16 ページ）
- Cisco フローティング L3Out について （28 ページ）

L3Out のインターフェイスの変更

GUI を使用した L3Out のインターフェイスの変更

この手順では、L3Out インターフェイスを変更します。

（注） フィールドに入力する手順は、必ずしも GUI に表示される順序と同じ順序でリストされているわけではありません。

始める前に

- [Cisco ACI] ファブリックがインストールされ、 [Cisco APIC]がオンラインで、 [Cisco APIC] クラスターが形成され、正常に動作していることを示します。
- 必要なファブリック インフラストラクチャ設定を作成できる [Cisco APIC] ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが [Cisco ACI] ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Outインターフェイスにポート チャネルが使用される場合に設定されます。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）] > [すべてのテナント（All Tenants）]**を選択します。

ステップ 2 作業ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、[tenant_name] **[ネットワーキング（Networking）] > [L3Out（L3Outs）] >** ***[L3Out]*** **> [論理ノード プロファイル（Logical Node Profiles）] >** ***[node_profile]*** **> [論理インターフェイス プロファイル（Logical Interface Profiles）]** を展開し、変更したいプロファイルを選択します。

ステップ 4 インターフェイス タイプ タブを選択します：**[ルーテッド サブインターフェイス（Routed Sub-Interfaces）]**、**[ルーテッド インターフェイス（Routed Interfaces）]**、**[SVI]**または**[フローティング SVI（Floating SVI）]**を選択します。

ステップ 5 既存のインターフェイスをダブルクリックして変更するか、**[作成（Create）]**（**[+]**）ボタンをクリックして、論理的なインターフェイス プロファイルに新しいインターフェイスを追加します。

ステップ 6 浮動 SVI 以外のインターフェイス タイプの場合は、次のサブステップを実行します。

a) **[パスタイプ（Path Type）]** フィールドで新しいインターフェイスを追加するには、適切なパス タイプを選択します。

ルーテッドサブインターフェイスまたはルーテッドインターフェイスタイプの場合、**[ポート（Port）]** または **[ダイレクト ポート チャネル（Direct Port Channel）]**を選択します。SVI インターフェイス タイプとして、**[ポート（Port）]**、**[ダイレクト ポート チャネル（Direct Port Channel）]**、または **[仮想ポート チャネル（Virtual Port Channel）]**を選択します。

b) **[ノード（Node）]** ドロップダウン リストから、ノードを選択します。

（注）
これは、非ポート チャネル パス タイプにのみ適用されます。 **[パスタイプ（Path Type）]** を **[ポート（Port）]**として選択した場合、この手順を実行します。それ以外の場合は、次のステップに進みます。

c) **[パス（Path）]** ドロップダウン リストからインターフェイス ID またはポート チャネル名を選択します。

インターフェイス ID の例は eth 1/1 です。ポート チャネル名は、各直接または仮想ポート チャネルのインターフェイス ポリシー グループ名です。

ステップ 7 フローティング SVI インターフェイス タイプの場合、**[アンカー ノード（Anchor Node）]** ドロップダウン リストから、ノードを選択します。

ステップ 8 （任意） **[説明（Description）]** フィールドに、L3Out インターフェイスの説明を入力します。

ステップ 9 ルーテッド サブインターフェイス、SVI およびフローティングSVI インターフェイス タイプの場合、**[カプセル化（Encap）]** ドロップダウンリストから、**[VLAN]** を選択し、このエントリの整数値を入力します。

ステップ 10 SVI および浮動 SVI インターフェイス タイプの場合は、次のサブステップを実行します：

a) **[カプセル化範囲（Encap Scope）]** ボタンで、レイヤ 3 Outside プロファイルに使用されるカプセル化の範囲を選択します。

- **[VRF]** : 特定の VLAN カプセル化の同じ VRF インスタンス内のすべてのレイヤ 3 外部で同じトランジット VLAN を使用します。これはグローバル値です。
- **[ローカル（Local）]** : レイヤ 3 外部ごとに一意のトランジット VLAN を使用します。

b) **[自動状態（Auto State）]** ボタンについては、この機能を有効にするか無効にするかを選択します。

- **[無効（disabled）]** : インターフェイスが対応する VLAN で動作していない場合、SVI がアクティブであることを意味します。
- **[有効（enabled）]** : VLAN インターフェイスが VLAN で複数のポートを有する場合、SVI は 浮動 SVI はVLAN のすべてのポートがダウンするとダウン状態になります。

c) **[モード（Mode）]** ボタンで、VLAN タギング モードを選択します。

ステップ 11 **[IPv4 プライマリ/IPv6 優先アドレス（IPv4 Primary / IPv6 Preferred Address）]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのプライマリ IP アドレスを入力します。

ステップ 12 **[IPv4 セカンダリ アドレス / IPv6 追加アドレス（IPv4 Secondary / IPv6 Additional Addresses）]** テーブルで、 **[+]** をクリックして、レイヤ 3 外側プロファイルにアタッチされているパスのセカンダリ IP アドレスを入力します。

ステップ 13 （任意） **[リンクローカル アドレス（Link-local Address）]** フィールドに、 IPv6 リンクローカル アドレスを入力します。これは、システムによって生成された IPv6 リンクローカルアドレスをオーバーライドします。

ステップ 14 **[MAC アドレス（MAC Address）]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスの MAC アドレスを入力します。

ステップ 15 **[MTU（バイト）（MTU（bytes））]** フィールドで、外部ネットワークの最大転送単位を設定します。範囲は 576 ～ 9216 です。値を継承する場合、フィールドに *[継承（inherit）]* を入力します。

ステップ 16 リスト **[ターゲット DSCP（Target DSCP）]** ドロップダウンリストで、レイヤ 3 アウトサイド プロファイルに接続されているパスのターゲット Differentiated Services Code Point（DSCP）を選択します。

ステップ 17 **[送信（Submit）]**をクリックします。

OSPF インターフェイス プロファイルの作成

OSPF インターフェイス プロファイルは、インターフェイスで OSPF を有効にします。オプションとして、OSPF インターフェイスプロファイルに OSPF インターフェイスポリシーとの関係を設定すれば、インターフェイスのプロパティをより詳細に制御できます。

[障害（Fault）]

次のようなシナリオでは障害が発生し、OSPF セッションがダウンします。

- KeyChain ポリシーの「Key」で提供されることになっているキー（キー文字列）で、事前共有キーが提供されていない
- KeyChain ポリシーでキー（キー文字列）が構成されていない

- 3DES や AES などのサポートされていない暗号化アルゴリズムを指定した。これらのアルゴリズムは、認証ではサポートされています。

キーの送信/受け入れライフタイムが期限切れになり、現用系のキーがなくなったためにOSPFセッションがダウンしても、障害は発生しません。OSPF インターフェイスの KeyChain の状態は「not-ready」（準備ができていない）状態になります。

始める前に

- Cisco ACI ファブリックが設置され、Cisco APIC がオンラインになっていて、Cisco APIC クラスタが形成されていて正常に動作していること。
- 必要なファブリック インフラストラクチャ構成を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Out インターフェイスにポート チャネルが使用される場合に構成されます。

手順

ステップ 1 メニューバーで、 **[テナント（Tenants）] > [すべてのテナント（All Tenants）]**を選択します。

ステップ 2 作業ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、 **[tenant_name] > [ネットワーキング（Networking）] > [L3Out（L3Outs）] > [L3Out（L3Out）] > [論理ノード プロファイル（Logical Node Profiles）] > [node_profile] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [OSPF インターフェイス プロファイル（OSPF Interface Profile）]**を展開します。

ステップ 4 **[名前（Name）]**フィールドに、OSPF インターフェイスの名前を入力します。この名前では最大 64 文字までの英数字を使用できます。

（注）
オブジェクトの作成後は、この名前は変更できません。

ステップ 5 [オプション] **[説明（Description）]**フィールドに、この OSPF インターフェイス プロファイルの説明を入力します。説明には最大 128 文字までの英数字を使用できます（省略も可）。

ステップ 6 ターゲット インターフェイス ポリシー名の値を入力します。この名前では最大 64 文字までの英数字を使用できます。オブジェクトの作成後は、この名前は変更できません。

ステップ 7 MD5 または簡易認証を使用して OSPF インターフェイスプロファイルを構成するには、次の手順を実行します。

a) **[OSPFv2 認証キー（OSPFv2 Authentication Key）]** フィールドに、認証キーを入力します。認証キーは、一種のパスワードで（最大 8 文字）、インターフェイスごとに割り当てることができます。そのインターフェイス上の認証キーは、各ルータ間で一致させる必要があります。

（注）

認証を使用するには、このインターフェイスのエリアに対する OSPF 認証タイプをシンプルに設定します（デフォルトはなしです）。

b) **[OSPFv2 認証キーを確認（Confirm OSPFv2 Authentication Key）]** フィールドに、認証キーを再入力します。

c) **[OSPFv2 認証キー ID（OSPFv2 Authentication Key ID）]** フィールドに、認証キー識別子を入力します。

d) OSPFv2 認証タイプ フィールドで、適切なオプションを選択します。

OSPF 認証タイプ。認証により、OSPF ネイバーを柔軟に認証できます。OSPF での認証を有効にすることにより、ルーティングの更新情報を安全な方法で交換できます。

（注）
認証を構成するときは、エリア全体を同じタイプの認証で構成する必要があります。

認証タイプは次のとおりです：

- **[なし（None）]**：認証は使用されません。
- **[シンプル（Simple）]**：認証キー、以前指定した **[OSPFv2 認証キー（OSPFv2 Authentication Key）]** を指定する必要があります。認証キーは、一種のパスワードで（最大 8 文字）、インターフェイスごとに割り当てることができます。そのインターフェイス
- **Md5**上の認証キーは、各ルータ間で一致させる必要があります。：パスワードをネットワークを介して渡しません、MD5 は、RFC 1321 で規定されたメッセージダイジェストアルゴリズムです。MD5 が最も安全な OSPF 認証モードと見なされています。認証を設定するときは、領域全体を同じタイプの認証で設定する必要があります。

デフォルトは、**[なし（None）]**です。

ステップ 8 KeyChain 認証を使用して OSPF インターフェイスプロファイルを構成するには、次の手順を実行します：

a) **[OSPFv2 キーチェーン ポリシー（OSPFv2 KeyChain Policy）]** フィールドで、OSPFv2 キーチェーン ポリシーを選択します。

OSPFv2 キーチェーン ポリシーは、簡易認証および MD5 認証とともに HMAC-SHA 認証をサポートします。このオプションを選択すると、同じキー チェーンの下に複数のキーを含めることができます。

セキュリティを強化するために、各キーの有効期間を指定して、キーのローテーションを設定できます。キーの有効期間が切れると、次のキーに自動的にローテーションされます。アルゴリズムを指定しなかった場合、OSPF はデフォルトの暗号化認証アルゴリズムである MD5 を使用します。

（注）
新しいキーが優先キーであり、既存のキーよりも優先されます。

（注）
レガシー ウェイ（ *[OSPFv2* 認証タイプ：*MD5* 認証/簡易認証（*OSPFv2 authentication type - MD5 authentication /Simple authentication* ）*]*を指定することで認証を構成または、 *[OSPFv2* キーチェーン ポリシー（*OSPFv2 keychain policy*）*]*を指定します。

キーチェーン ポリシーを構成すると、選択済みの認証タイプは上書きされます。

ステップ 9 （OSPFv3 にのみ適用） **[OSPFv3 IPsec ポリシー（OSPFv3 IPsec Policy）]**：OSPFv3 IPsec ポリシーを L3Out インターフェイスに関連付けるには、ドロップダウン リストから IPsec ポリシーを選択します。OSPFv3 IPsec ポリシーの作成については、 [OSPF IPsec ポリシーの作成（Create an OSPF IPsec Policy）] 手順を参照してください。

次のタスク

OSPFv2 KeyChain のローテーションを指定するには、 キー ポリシーの作成 （6 ページ）を参照してください。

キー ポリシーの作成

始める前に

OSPFv2 インターフェイス プロファイルが作成されていることを確認します。次の情報を参照してください。 OSPF インターフェイス プロファイルの作成 （3 ページ） を参照してください。

手順

ステップ 1 メニューバーで **[テナント（Tenants）] > [すべてのテナント（All Tenants）]**をクリックします。

ステップ 2 作業ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで **[ポリシー（Policies）] > [プロトコル（Protocol）] > [キーチェーン（KeyChains）]**に移動します。

ステップ 4 次を右クリックします。 **[キーチェーン（KeyChains）]**次を選択します。 **[キー ポリシーの作成（Create Key Policy）]**そして、次のステップを実行します：

a) ポリシーの名前を入力し、必要に応じて説明を追加します。

b) **[キー ID（Key ID）]** フィールドにキー ID 番号を入力します。

c) **[事前共有キー（Pre-Shared Key）]** フィールドに事前共有キーの情報を入力します。

d) **[暗号化アルゴリズム（Cryptographic Algorithm）]** フィールドでアルゴリズムを入力します。

e) **[開始時刻（Start Time）]** フィールドに開始時刻を **YYYY-MM--DD- HH-MM-SS** 形式で指定します。

f) **[終了時間（End Time）]** フィールドで終了時刻を **YYYY-MM--DD- HH-MM-SS** 形式で指定します。

g) **[キー受け入れライフタイムの開始時刻（Key accept lifetime start time）]**フィールドに開始時刻を **YYYY-MM--DD- HH-MM-SS** 形式で指定します。

これはローテーション キーです。各キーの有効期間を指定します。キーのライフタイムが期限切れになると、次のキーに自動的にローテーションされます。アルゴリズムを指定しない場合、OSPF はデフォルトの暗号化認証アルゴリズムである MD5 を使用します。

このフィールドは OSPFv3 IPSec ポリシーには適用されません。

（注）
新しいキーが優先キーであり、既存のキーよりも優先されます。

h) **[キー受け入れライフタイムの終了時刻（Key accept lifetime end time）]**フィールドで終了時間を **YYYY-MM--DD- HH-MM-SS** 形式で指定します。

このフィールドは OSPFv3 IPSec ポリシーには適用されません。

ステップ 5 **[送信（Submit）]**をクリックします。

OSPF IPsec ポリシーの作成

Cisco APIC リリース 6.1（2）以降では、OSPFv3 セッションの暗号化と認証がサポートされています。この手順を使用します

（注） OSPFv3 はインフラ テナントではサポートされていません。 OSPF IPSec ポリシーのサポートは、ユーザ テナントのみを対象としています。

始める前に

キーチェーン ポリシーを作成します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]**> *[*テナント名（*tenant name*）*]*。

ステップ 2 左側のナビゲーション ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[OSPF]**> **[OSPF IPSec]**に移動します。

ステップ 3 **[IPSec 認証ポリシーを作成（Create IPSec Authentication Policy）]** ウィンドウで、次の詳細を入力します：

- 名前：IPSec ポリシーの名前。
- 説明：この IPSec ポリシーの説明。
- IPセキュリティ プロトコル：認証ヘッダー（AH）またはカプセル化セキュリティ ペイロード（ESP）のいずれかを選択します。

  認証ヘッダーを選択した場合は、認証のみがサポートされます。ESP を選択した場合、使用可能なオプションは認証、暗号化、または両方（認証と暗号化）です。

  サポートされているキーチェーンアルゴリズム：

  - 認証ヘッダー：MD5（デフォルト）、HMAC-SHA1。
  - カプセル化セキュリティ プロトコル：認証用：HMAC-SHA1。暗号化の場合：3DES（デフォルト）、AES。

  （注）

アルゴリズムを選択しないか、サポートされていないアルゴリズムを選択すると、デフォルトが自動的に選択されます。

- セキュリティ パラメータ インデックス：IPSec プロトコルを作成するための一意の値。ドロップダウン リストから値を選択します。サポートされている範囲は 256 ～ 4294967295 です。
- OSPFv3 認証キーチェーン：ドロップダウン リストからキーチェーン値を選択します。IP セキュリティ プロトコル フィールドで AH オプションを選択した場合、このフィールドは必須です。フィールドを空白のままにすると、障害が生じます。

  障害が実際に生じたかを確認するには、OSPF インターフェイス プロファイル画面に移動し、障害タブをクリックします。**[障害（Fault）]** タブに表示されるフィールドとアイコンについて説明します。
- OSPFv3 暗号化キーチェーン：ドロップダウン リストからキーチェーン値を選択します。 **[IP セキュリティ プロトコル（IP Security Protocol）]** フィールドで AH オプションを選択した場合、このフィールドは適用外になります。IP セキュリティ プロトコル フィールドで ESP オプションを選択した場合は、 **[認証キーチェーン（Authentication Keychain）]** フィールドまたは **[暗号化キーチェーン（Encryption Keychain）]** フィールドに値を入力する必要があります。

ステップ 4 **[送信（Submit）]** をクリックします。

SSH またはコンソール セッション上のスイッチで **show ipv6 ospfv3 interface***interface-id* コマンドを使用すれば、作成された IPSec ポリシーを確認できます。

ステップ 5 作成した OSPFv3 IPSec ポリシーを L3Out インターフェイスに関連付けるには、 「OSPF インターフェイス プロファイルの作成」の手順のステップ 9 を参照してください。

OSPF タイマー ポリシーを作成

OSPF タイマーは、プロトコル メッセージおよび最短パス優先（SPF）計算の動作を制御します。VRF で使用されるこのポリシーを構成するには、次の手順を活用。

始める前に

OSPFv2 インターフェイス プロファイルが作成されていることを確認します。詳細については、 OSPF インターフェイス プロファイルの作成 （3 ページ） を参照してください。

手順

ステップ 1 メニューバーで、 **[テナント（Tenants）] > [OSPF）]> [OSPF] > [OSPFタイマー（OSPF Timers）]** を選択します。

ステップ 2 作業ペインで、テナントの名前をダブルクリックします。

ステップ 3 **[名前（Name）]**フィールドに、コンテキストレベルの OSPF ポリシー名を入力します。この名前では最大 64 文字までの英数字を使用できます。

（注）
オブジェクトの作成後は、この名前は変更できません。

ステップ 4 [オプション] **[説明（Description）]**フィールドに、この OSPF インターフェイス プロファイルの説明を入力します。説明には最大 128 文字までの英数字を使用できます（省略も可）。

ステップ 5 **[帯域幅のリファレンス（Bandwidth Reference）]** フィールドに、 OSPF 帯域幅のリファレンスを入力します。これは、インターフェイスのデフォルトメトリックを計算するために使用されます。範囲は 0 ～ 40000 です。デフォルト値は 40000 です。

ステップ 6 **[アドミニストレーティブ ディスタンス優先設定（Admin Distance Preference）]** フィールドに、優先するアドミニストレーティブ ディスタンスを入力します。アドミニストレーティブ ディスタンスとは、2 つの異なるルーティング プロトコルから同じ宛先に向かう複数のルートが存在する場合に、ルータが最適なパスを選択するために使用する機能です。アドミニストレーティブ ディスタンスでは、ルーティング プロトコルの信頼性が定義されます。各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して、信頼性の高いプロトコルから低いプロトコルへの順序で優先順位が付けられます。有効値は 1 ～ 255 です。デフォルト値は 110 です。

ステップ 7 **[最大 ECMP（Maximum ECMP）]** フィールドに、 OSPF プロトコルの最大 ECMP を入力します。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。

ステップ 8 **[制御ノブ（Control Knobs）]** フィールドで、次の OSPF ポリシー制御タイプのいずれかを入力します。

- **[ルータ IDの名前ルックアップを有効（Enable name lookup fo router IDs）]**
- **[プレフィックスの抑制（Prefix suppression）]** : プレフィックスはアドバタイズされません。

ステップ 9 **[グレースフル リスタート制御（Graceful Restart Controls）]** チェックボックスをオンにしてグレースフル リスタート、または、ノンストップ フォワーディング（NSF）を有効にします。これは、OSPF がデータ転送パス上に存在し続けることを有効にします。

ステップ 10 **[初期 SPF スケジュールの遅延間隔（Ms）（Initial Spf Schedule Delay Interval (Ms)）]** フィールドに、SPFスケジュールの初期遅延間隔を入力します。期間とは、最初の SPF 計算が実行されるまで待機する時間のことです。最初の計算を行うたびに、期間は、その前の期間の 2 倍の長さになり、指定された最大待機期間に達するまでそれが行われます。指定できる範囲は 1 ～ 600000 です。デフォルト値は 200 です。

ステップ 11 **[SPF 計算の最小保留時間 (Ms)（Minimum Hold Time Between Spf Calculations (Ms)）]** フィールドで SPF 計算間の最小保留時間を入力します。期間とは、初期間隔が発生した後の SPF 計算が実行されるまで待機する最小限の時間のことです。最初の計算を行うたびに、期間は、その前の期間の 2 倍の長さになり、指定された最大待機期間に達するまでそれが行われます。指定できる範囲は 1 ～ 600000 です。デフォルト値は 1000 です。

ステップ 12 **[SPF 計算間の最大待機時間（Ms）（Maximum Wait Time Between Spf Calculations (Ms)）]** フィールドで SPF 計算間の最大間隔を入力します。最初の計算を行うたびに、期間は、その前の期間の 2 倍の長さになり、指定された最大待機期間に達するまでそれが行われます。指定できる範囲は 1 ～ 600000 です。デフォルト値は 5000 です。

ステップ 13 **[LSA グループ ペーシング間隔（Secs）（LSA Group Pacing Interval (Secs)）]** フィールドで LSA がグループ化されリフレッシュ、チェックサム算出、またはエージングされる間隔を入力くます。LSAグルー

プ ペーシングの期間は、ルータが処理する LSA 数に反比例します。たとえば、約 10,000 の LSA がある場合は、ペーシング間隔を短くする必要があります。小さなデータベース（40 ～ 100 LSA）を使用する場合は、ペーシング インターバルを10 ～ 20 分に増やす必要があります。有効な範囲は 1 ～ 1800 秒です。デフォルト値は 10 秒です。

ステップ 14 **[LSA 生成スロットル開始待機間隔（LSA Generation Throttle Start Wait Interval (Ms)）]** フィールドに、LSA 間の生成スロットル開始待機間隔を入力します。これは、同じLSAを受け入れるための最小間隔です。同じLSA のインスタンスが、設定されている間隔が経過する前に到着した場合、そのLSA はドロップされます。指定できる範囲は 0 ～ 5000 です。デフォルト値は 0 です。

ステップ 15 **[LSA生成スロットル保留間隔（Ms）（LSA Generation Throttle Hold Interval (Ms)）]** フィールドに、LSA生成に対する後続のレート制限時間の計算に使用される増分時間（ミリ秒単位）を入力します。スロットル間隔の範囲は 50 ～ 30000 です。デフォルト値は 5000 です。

ステップ 16 **[LSA 生成スロットル最大間隔（Ms）（LSA Generation Throttle Maximum Interval (Ms)）]** フィールドに、 LSA生成の後続のレート制限時間を計算するために使用される最大時間（ミリ秒単位）を入力します。範囲は 50 ～ 30000 です。デフォルト値は 5000 です。

ステップ 17 **[LSA の最小到着間隔（Ms）（Minimum Interval Between Arrival of a LSA (Ms)）]** フィールドに、 ソフトウェアが Open Shortest Path First（OSPF）ネイバーから同じリンクステートアドバタイズメント（LSA）を受け入れる最小間隔を入力します。同じ LSA とは、同じ LSA ID 番号、LSA タイプ、およびアドバタイズ ルータ ID を含む LSA インスタンスです。同じ LSA のインスタンスが、設定されている間隔が経過する前に到着した場合、ソフトウェアは、LSA をドロップされます。範囲は 10 ～ 600000 です。デフォルト値は 1000 です。

ステップ 18 **[非自己生成 LSA の最大数（Maximum Number of Not Self-generated LSAs）]** フィールドで非自己生成 LSA の最大数を入力します。デフォルト値は 20000 です。

ステップ 19 **[LSA 最大スリープ無視カウント間隔（ignore-time）（LSA Maximum Sleep Ignore Count Interval (ignore-time)）]** LSA 制限を超えた後、OSPF プロセスが無視状態を維持する時間を分単位で指定します。

ステップ 20 **[LSA 最大スリープ無視カウント（ignore-count）（LSA Maximum Sleep Ignore Count (ignore-count)）]** フィールドで、手動リカバリが必要になる前に、OSPFプロセスが無視状態になることができる最大回数を設定します。

ステップ 21 **[LSA スリープ数リセット間隔（reset-time）（LSA Sleep Count Reset Interval (reset-time)）]** フィールドで、 OSPFプロセスが正常に動作して無視状態カウンタをゼロにリセットする時間を分単位で指定します。

ステップ 22 **[LSA しきい値（パーセンテージ）（LSA Threshold (percentage)）]** フィールドに、合計しきい値最大のパーセンテージで表される LSA の数を入力します。デフォルト値は 75% です。

ステップ 23 **[LSA 最大アクション数（LSA Maximum Action）]**フィールドで、**[ログ（Log）]**または**[拒否（Reject）]** オプションのいずれかを選択します。

ステップ 24 **[送信（Submit）]**をクリックします。

次のタスク

新しく作成された OSPF タイマー ポリシーを展開するには、**[テナント（Tenants）] > [ネットワーキング（Networking）] > [VRF] > [ポリシー（Policy）] > [OSPF タイマー（OSPF Timers）]** へ移動し、それを VRF に関連付けます。

OSPF リンク ステート データベース オーバーロードの防止

OSPFリンクステートデータベース オーバーロード保護機能を使用すると、特定のOpen Shortest Path First（OSPF）プロセスに対する非自己生成リンクステート アドバタイズメント（LSA）の数を制限できます。OSPFドメイン内の他のルータによって生成される過剰なLSA により、ルータのCPUおよびメモリ リソースが実質的に消費される可能性があります。

OSPF リンクステート データベース オーバーロードの防止の前提条件

ネットワークではOSPF が実行されていることが前提となります。

OSPF リンク ステート データベース オーバーロードの防止の利点

OSPF リンクステート データベース オーバーロード保護機能は、特定のOSPFプロセスに対して非自己生成LSAの数を制限するためのメカニズムをOSPF レベルで提供します。ネットワーク内の他のルータの設定が正しくない場合、たとえば、大量のプレフィックスを再配布するために大量の LSA が生成されることがあります。この保護メカニズムは、ルータが大量の LSA を受信することを防ぎ、 CPUおよびメモリの不足が発生するのを防ぎます。

OSPF リンク ステート データベース オーバーロードの防止

OSPFリンクステートデータベース オーバーロード保護機能がイネーブルになっている場合、ルータは受信した（非自己生成）LSA 数をカウントします。LSA の構成されたしきい値数に達すると、 **非自己発信LSAの数 < > が許容制限を超えました <>** 説明とともに障害が APIC で発生します。構成されているLSAの最大数を超えると、ルータがNotification（通告）を送信します。1 分経過しても受信 LSA 数が構成されている最大値よりも大きい場合、OSPF プロセスはすべての隣接関係を停止し、OSPF データベースをクリアします。この無視ステートでは、この OSPF プロセスに属する任意のインターフェイスで受信されたすべての OSPF パケットは無視され、これらのどのインターフェイスでも OSPF パケットは生成されません。 **[LSA 最大スリープ無視カウント間隔（LSA Maximum Sleep Ignore Count Interval）]**（`ignore-time`）フィールドで構成された期間、 OSPF プロセスは無視状態のままになります。OSPFプロセスが無視状態になるたびに、カウンタが増分されます。このカウンタが **[LSA 最大スリープ無視カウント（LSA Maximum Sleep Ignore Count）]**（`ignore-count`）フィールドで構成された値を超えた場合、 OSPF プロセスは永続的に無視状態のままになり、 OSPF プロセスをこの状態から戻すには手動の介入が必要です。 **[LSA スリープ数リセット間隔（LSA STEP Count Reset Interval）]**（`reset-time`）フィールドで指定された時間、OSPFプロセスが正常に動作すると、無視状態カウンタは 0 にリセットされます。

LSA 最大アクション（LSA Maximum Action）が **Log** （警告のみ）に設定されている場合、LSA の最大制限を超過しても、隣接関係に影響が及ばなければ、 OSPFプロセスによって障害が記録されます。

（注） 永続的な無視の状態から回復するには、次のいずれかの手動による介入が必要です：

1. L3Out でOSPFプロセスを無効にしてから再度有効にします（ユーザーテナントにある場合）。
2. プロセスを再起動します（例： `kill -9 $( <ospf>の pid)`。
3. デバイスをリロードします。

OSPF 最大メトリック

OSPF Max-Metric 機能により、ネットワーク内のルーティング情報のフローが制御されます。この機能により、ルータはローカルで生成されたリンクステートアドバタイズメント（LSA）を最大メトリックでアドバタイズできます。これにより、このルータがデータ トラフィックの中継パスとして望ましくない状態になります。このアプローチは、動作可能になるまでデバイスが中継トラフィックに選択されないようにするため、スイッチのリロード時に特に役立ちます。

OSPF 最大メトリック ポリシーのガイドライン

OSPF 最大メトリック ポリシーの構成を行うときは、次の注意事項に従ってください：

- common またはユーザー テナントの下に OSPF max-metric ポリシーを作成します。
- OSPF Max-Metric ポリシーを使用すると、外部 LSA、スタブ リンク、サマリー LSA などの制御を選択でき、1 ～ 16,777,215 の範囲で max-metric 値を指定できます。この最大メトリック値は、外部 LSA およびサマリー LSA にのみ適用されます。スタブ ネットワーク用のルータ LSA およびルータLSA は、常に 65,535 の固定の最大メトリック値でアドバタイズされます。
- OSPF Max-Metric ポリシーが、External LSAs、Stub Links、または Summary LSAs コントロールを選択せずに有効になった場合は、非スタブ ネットワークのルータ LSA だけが max-metric 値でアドバタイズされます。
- On Startup 制御が有効である場合、 OSPF最大メトリック ポリシーは、スイッチの起動後、設定された起動間隔の間だけアドバタイズされます。On Startup が有効になっていない場合、構成された最大メトリックは、 VRF 内のすべての OSPF 対応ボーダー リーフからアドバタイズされます。
- OSPF max-metric ポリシーを、max-metric を有効にする必要がある VRF に関連付けます。
- OSPF max-metric ポリシーは infra テナントではサポートされていません。
- ボーダー リーフ スイッチにのみ OSPF max-metric ポリシーを展開します。
- PE ではオーバーロード モードがデフォルトで暗黙的に有効になっているため、この機能はインフラテナントの overlay-1 VRF ではサポートされません。

OSPF max-metric ポリシーの制限

OSPF Max-Metric ポリシーを構成する場合は、次の制限事項に注意してください：

- OSPF max-metric policy 内の **wait-for-bgp** オプションは、 ACI の BGP 機能の制限によりサポートされていません。
- OSPF 最大メトリック ポリシーは、リリース 6.1.4 の OSPFv3 ではサポートされていません。

GUI を使用して OSPF 最大メトリック ポリシーを作成

短期間だけ、ルータ経由の OSPF トラフィックを制限する場合は、このタスクを使用します。

GUI を使用してOSPF Max-Metric ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]**を選択します。

ステップ 2 ナビゲーション ペインで、*[Tenant_name]* > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[OSPF]** を展開し、**[OSPF Max-Metric]** を右クリックし、**[OSPF 最大メトリック ポリシーの作成（Create Max-Metric OSPF Policy）]**を選択します。

[ドメイン/ VRF ごとの最大メトリック リンク ステート アドバタイズメントの作成（Create Max-Metric Link State Advertisement per Domain/VRF）] ダイアログボックスが表示されます。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 必要な最大メトリック制御を構成します。

a) **[外部 LSA（External LSAs）]** チェックボックスをオンにして、外部 LSA を最大メトリックに設定します。

b) **[起動時（On Startup）]** チェックボックスをオンにして、スタートアップ時に最大メトリックをアドバタイズするようにルータを設定します。

c) **[スタブ リンク（Stub Links）]** チェックボックスをオンにして、スタブリンクを最大メトリックに設定します。

d) **[集約 LSA（Summary LSAs）]** チェックボックスをオンにして、サマリー LSA を最大 メトリックに構成します。

外部 LSA、スタブ リンク、またはサマリー LSA を選択しない場合、システムはルータ LSA に対してのみ最大メトリックをアドバタイズします。これらの制御のいずれかが有効になっている場合、対応する LSA およびルータ LSA が最大メトリックでアドバタイズされます。

ステップ 5 **[外部 LSA の最大メトリック値（Maximum metric value for external LSAs）]** フィールドに値を入力して最大メトリック値を指定します。

デフォルト値は 65,535 です。範囲は 1 ～ 16777215 です。ルータLSA は、max-metric が有効になっている場合、常に 65,535 のメトリック値でアドバタイズされます。

ステップ 6 **[サマリー LSA の最大メトリック値（Maximum metric value for summary LSAs）]** フィールドを選択し、集約 LSA の最大メトリック値を指定します。

デフォルト値は 65,535 です。有効な範囲は 1 ～ 16777215 です。

ステップ 7 **[起動間隔時間（秒）（Startup Interval Time (in secs)）]** フィールドで、最大メトリックをアドバタイズする時間間隔を指定します。

デフォルト値は 600 秒です。値の範囲は 5 ～ 86,400 秒です。

ステップ 8 **[送信（Submit）]**をクリックします。

作成された OSPF 最大メトリック ポリシーが、**[プロトコル（Protocol）]** > **[OSPF]** > **[OSPF 最大メトリック（OSPF Max-Metric）]**の下で表示されます。

VRF の作成時にOSPF最大メトリック ポリシーを作成することもできます。**[VRF の作成（Create VRF）]** ウィザードのステップ1で、**[OSPF ポリシーを構成（Configure OSPF Policies）]** チェックボックスをオンにします。ウィザードのステップ 2 で、**[OSPF 最大メトリック ポリシーの作成（Create Max-Metric OSPF Policy）]** を選択します。これは、**[OSPF 最大メトリック（OSPF Max-Metric）]** ドロップダウンリストにあります。

GUI を使用して OSPF 最大メトリック ポリシーを VRF に関連付ける

OSPF 最大メトリック ポリシーを VRF に関連付けるには、 GUI を使用して次の手順を実行します。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]**を選択します。

ステップ 2 ナビゲーション ペインで、*[Tenant_name]* > **[ネットワーキング（Networking）]** > **[VRF]** [VRF] を選択します。

右側のペインで、選択した VRF の詳細を確認できます。

ステップ 3 **[ポリシー（Policy）]** タブをクリックします。

ステップ 4 **O[SPF Max-Metric]** ドロップダウンリストで、 OSPF max-metric ポリシーを選択します。

ステップ 5 OSPF Max-Metric ポリシーをVRFに関連付けをするために **[送信（Submit）]** をクリックします。

関連付けられた OSPF 最大メトリック ポリシーが **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[OSPF]**削除された場合、障害が発生します。

CLI を使用した OSPF 最大メトリック ポリシー構成を確認

CLI を使用して OSPF 最大メトリック ポリシーの構成を確認するには、次の手順に従います。

手順

特定のVRFインスタンス内のOSPF情報を表示すrには、 **show ip ospf vrf** コマンドを実行します。

例：

```
nextaci1-leaf1# show ip ospf vrf ospf_max-metric:ospf_vrf_backbone
 Routing Process default with ID 101.101.101.101 VRF ospf_max-metric:ospf_vrf_ba
ckbone
 Routing Process Instance Number 1
 Stateful High Availability enabled
 Graceful-restart helper mode is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
 Maximum number of non self-generated LSA allowed 20000
    (feature configured but inactive)
    Current number of non self-generated LSA 2
    Threshold for warning message 75%
    Ignore-time 5 minutes, reset-time 10 minutes
    Ignore-count allowed 5, current ignore-count 0
 Table-map using route-map exp-ctx-2818053-deny-external-tag
 Redistributing External Routes from
   static route-map exp-ctx-st-2818053
   direct route-map exp-ctx-st-2818053
   bgp-100 route-map exp-ctx-proto-2818053
   eigrp-default route-map exp-ctx-proto-2818053
   coop route-map exp-ctx-st-2818053
 Administrative distance 110
 Reference Bandwidth is 40000 Mbps
 SPF throttling delay time of 200.000 msecs,
   SPF throttling hold time of 1000.000 msecs,
   SPF throttling maximum wait time of 5000.000 msecs
 LSA throttling start time of 0.000 msecs,
   LSA throttling hold interval of 5000.000 msecs,
   LSA throttling maximum wait time of 5000.000 msecs
 Minimum LSA arrival 1000.000 msec
 LSA group pacing timer 10 secs
 Maximum paths to destination 8
 Originating router LSA with maximum metric
   Condition: Always
 Number of external LSAs 1, checksum sum 0x5c0e
 Number of opaque AS LSAs 0, checksum sum 0
```

L3Out の SVI のカスタマイズ

SVI 外部カプセル化の範囲

SVI 外部カプセル化の範囲について

レイヤ 3 アウト構成のコンテキストでは、スイッチ仮想インターフェイス（SVI）は ACI リーフ スイッチとルータ間に接続性を提供するように構成されます。

デフォルトで単一のレイヤ 3 アウトが SVI インターフェイスで構成されている場合、VLAN のカプセル化はファブリック内の複数のノードに範囲が及びます。これは、図で示されるように SVI インターフェイスが同じ外部カプセル化（SVI）を使用する限り、レイヤ 3 アウト SVI が展開されているファブリックで、ACI ファブリックがすべてのノード上に同じブリッジ ドメイン（VXLAN VN）を構成するため発生します。

ただし、異なるレイヤ 3 アウトが展開されている場合、同じ外部カプセル化 (SVI) を使用している場合でも ACI ファブリックは異なるブリッジ ドメインを使用します。

図 *1:* ローカル範囲のカプセル化と *1* 個のレイヤ *3* アウト

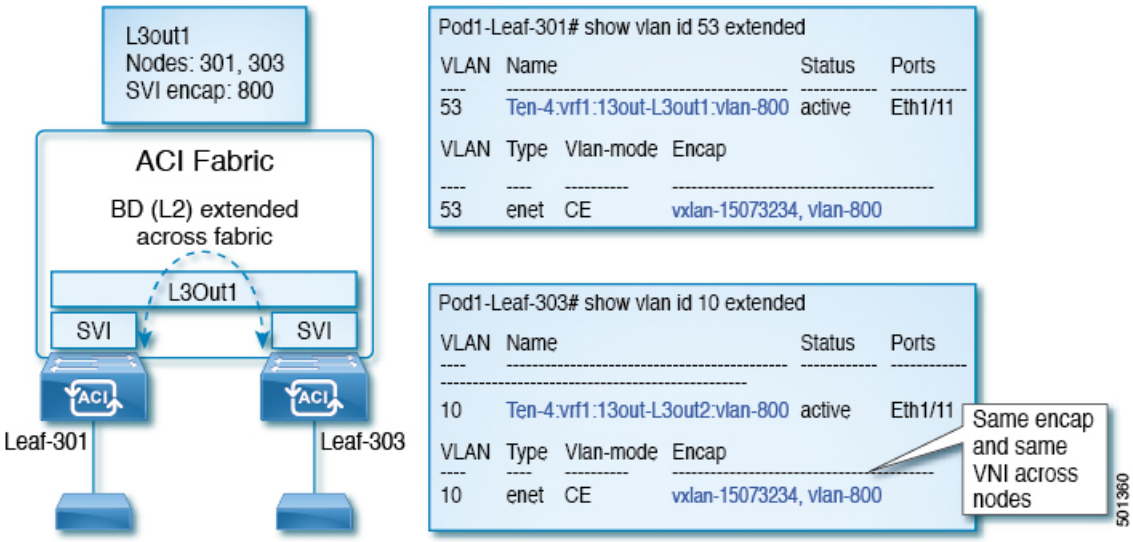
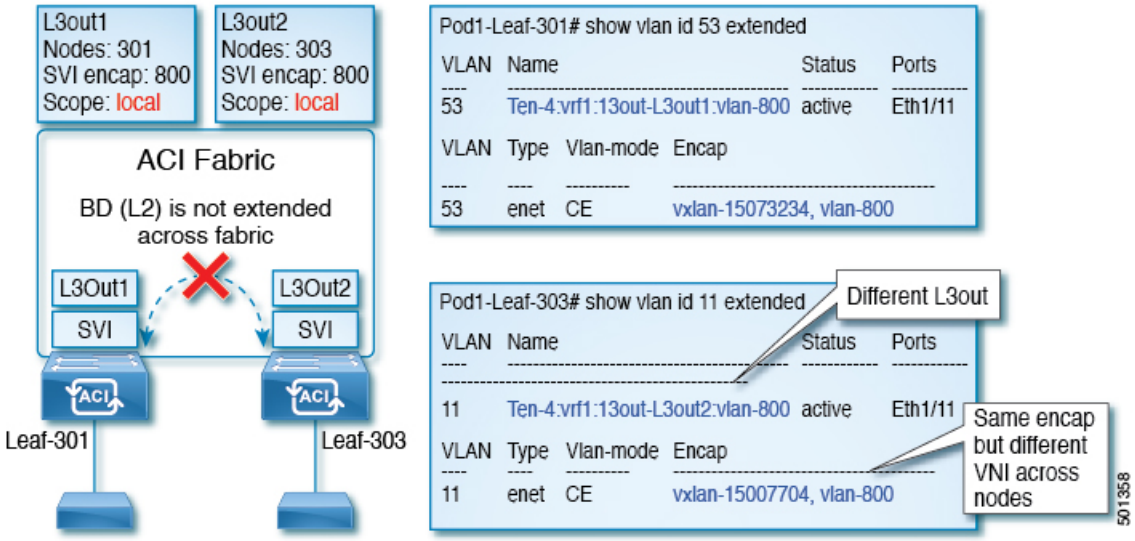


図 *2 :* ローカル範囲のカプセル化と *2* 個のレイヤ *3* アウト

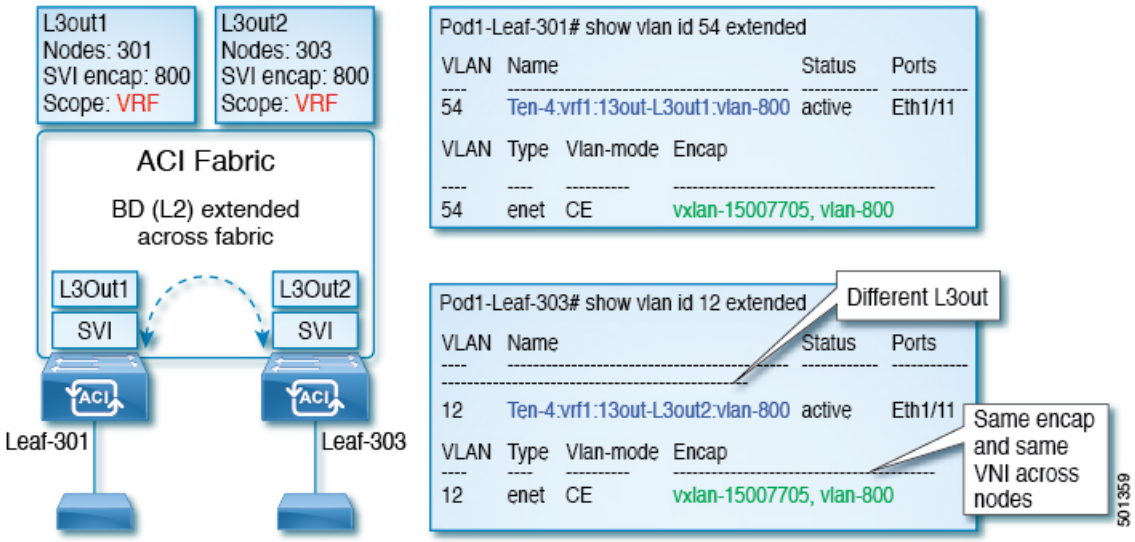


Cisco APIC リリース 2.3 以降、同じ外部カプセル化（SVI）を使用して、2 個以上のレイヤ 3 アウトを展開する場合の動作を選択できるようになりました。

カプセル化の範囲は、ローカルまたは VRF として構成できます。

- ローカル範囲（デフォルト）：例の動作が ローカル範囲のカプセル化と *2* 個のレイヤ *3* アウトというタイトルの図に表示されます。
- VRF 範囲：ACI ファブリックが、同じ外部カプセル化（SVI）が展開されているすべてのノードとレイヤ 3 アウト上で同じブリッジ ドメイン（VXLAN VNI）を構成します。次のタイトルの図の例を参照してください。 *VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト。

図 *3 : VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト



カプセル化スコープ構文

レイヤ 3 Out プロファイルで使用されるカプセル化の範囲を設定するためのオプションは次のとおりです。

- **CTX**特定の VLAN のカプセル化の同じ VRF に、すべてのレイヤ 3 が記録されるで同じ外部 SVI。これはグローバル値です。
- **ローカル** : レイヤ 3 Out ごとの一意の外部 SVI。これはデフォルト値です。

CLI、API、および GUI 構文間のマッピングは次のとおりです。

表 *1:* カプセル化スコープ構文

CLI	API	GUI
l3out	local	local
vrf	ctx	VRF

（注） カプセル化の範囲を設定する CLI コマンドでは、名前付きのレイヤ 3 アウト設定、VRF が設定されている場合にのみサポートされます。

SVI 外部カプセル化の範囲のガイドライン

SVI 外部カプセル化の範囲を使用する際には、次のガイドラインに従ってください:

- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の OSPF エリアが異なっている必要があります。
- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の BGP ピア設定が異なる必要があります。

GUI を使用して SVI 外部カプセル化の範囲の構成

始める前に

- テナントと VRF が構成されています。
- L3Out が構成されていて、L3Out で論理ノード プロファイルが構成されています。

手順

ステップ 1 メニュー バーで、 > **[テナント（Tenants）]** > ***[tenant-name]***をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[LogicalNodeProfile_name]*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]**をクリックします。

ステップ 3 次に **ナビゲーション** ペインで、**[論理インターフェイス プロファイル（Logical Interface Profiles）]**を右クリックし、**[インターフェイス プロファイルの作成（Create Interface Profile）]**をクリックします。

ステップ 4 **[インターフェイス プロファイルの作成（Create Interface Profile）]** ダイアログ ボックスで、次の操作を実行します：

a) **[ステップ 1 アイデンティティ（STEP 1 Identity）]** 画面の **[名前（Name）]** フィールドに、インターフェイス プロファイルの名前を入力します。

b) 残りのフィールドに、適切なオプションを選択し、**[次へ（Next）]**をクリックします。

c) **[ステップ 2 プロトコル プロファイル（Step 2 Protocol Profiles）]** 画面、目的のプロトコルを選択するには、プロファイルの詳細、および **[次へ（Next）]**をクリックします。

d) **[ステップ 3 のインターフェイス（Step 3 Interfaces）]** 画面で、**SVI** タブをクリックし、**+** アイコンをクリックして **[SVI の選択（Select SVI）]** ダイアロ グボックスを開きます。

e) **[インターフェイスの指定（Specify Interface）]** エリアで、目的、さまざまなフィールド値を選択します。

f) **[カプセル化範囲（Encap Scope）]** フィールドで、目的のカプセル化範囲の値を選択します。 **[OK]**をクリックします。

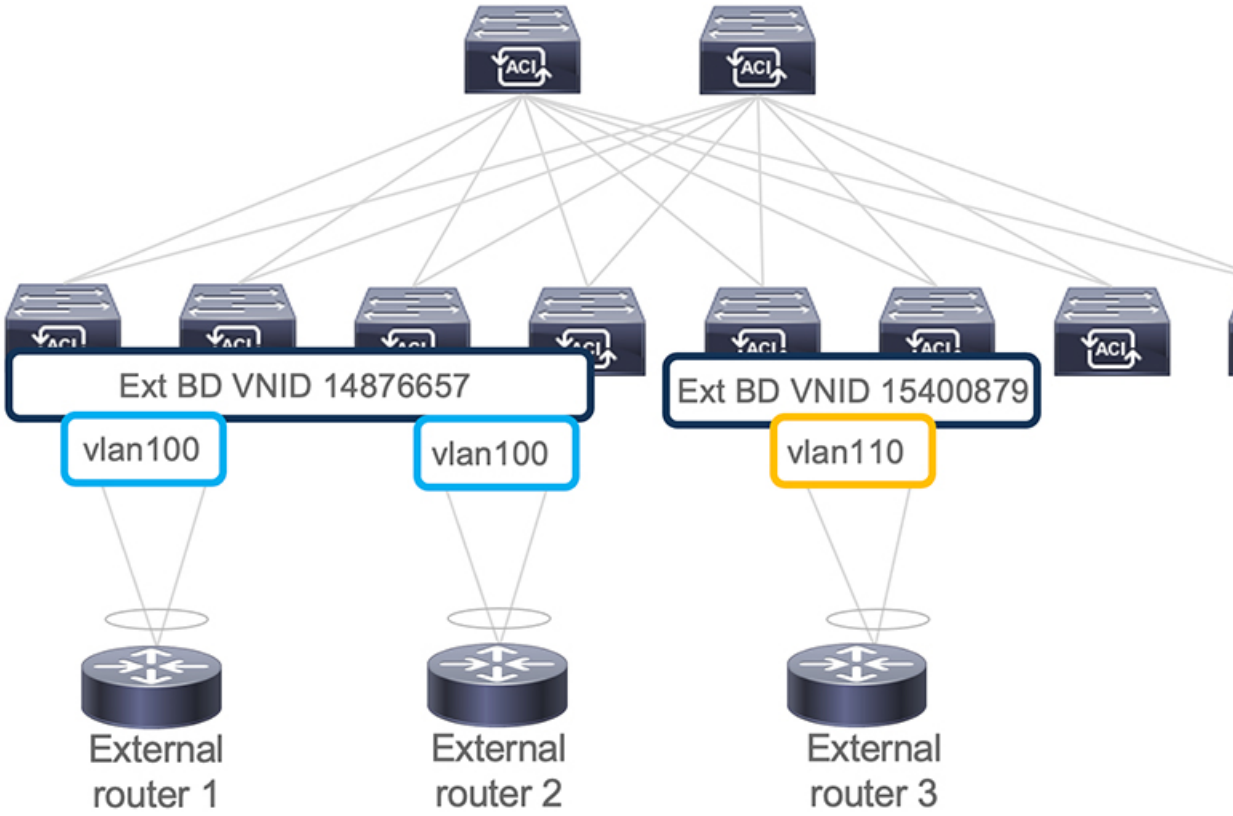
デフォルト値は、**[ローカル（Local）]**です。

SVI 外部のカプセル化の範囲は、指定されたインターフェイスで設定されます。

SVI での複数の L3Out のカプセル化のサポート

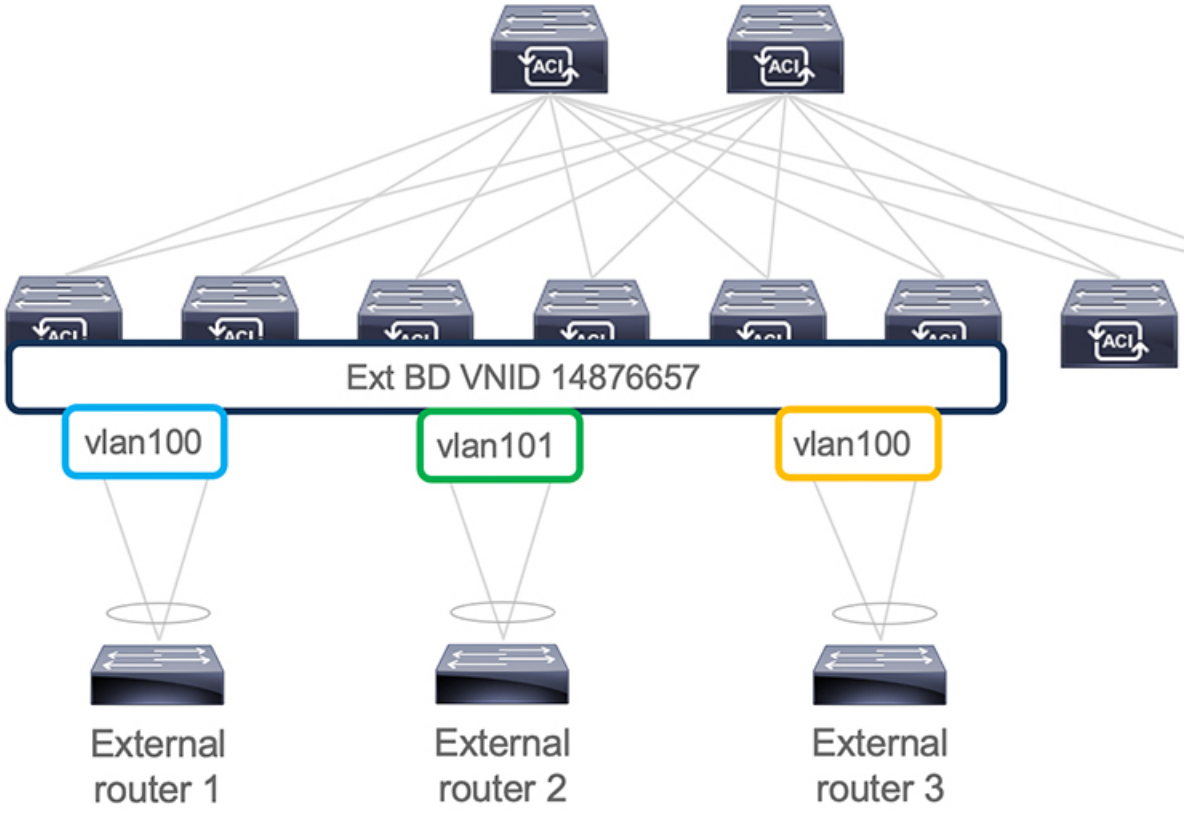
同じカプセル化 VLAN を使用する異なるリーフ スイッチ上の SVI インターフェイスで L3Out が設定されている場合、SVI VLAN は同じ VXLAN ネットワーク識別子（VNID）にマッピングされます。これにより、ファブリック全体に単一のブリッジ ドメイン（外部ブリッジ ドメイン）とブロードキャスト ドメインが形成されます。次の図に示すように、異なる VLAN で設定された SVI インターフェイスは、別個の外部ブリッジ ドメインを形成します。リリース 5.2(3) より前は、異なるスイッチ上に異なるカプセル化 VLAN を持つ単一の外部ブリッジ ドメインを作成することはできませんでした。

図 *4 :* カプセル化が異なる外部ブリッジ ドメインに関連付けられた個別の *VNID*（*ACI 5.2(3)* より前のリリース）。



リリース 5.2(3) では、異なるリーフ スイッチ上の異なるカプセル化 VLAN で構成できる単一の外部ブリッジを構成するためのサポートが追加されました。複数カプセル化のサポート機能では、フローティング SVI オブジェクトを使用して、フローティング L3Out の外部ブリッジ ドメインを定義するか、または外部ブリッジ グループ プロファイルを使用して、通常の L3Out の外部ブリッジ ドメインを定義します。この機能の使用例としては、同じ VLAN がすでに使用されている可能性があるため、異なるリーフ スイッチで同じ VLAN を使用できない場合があります。

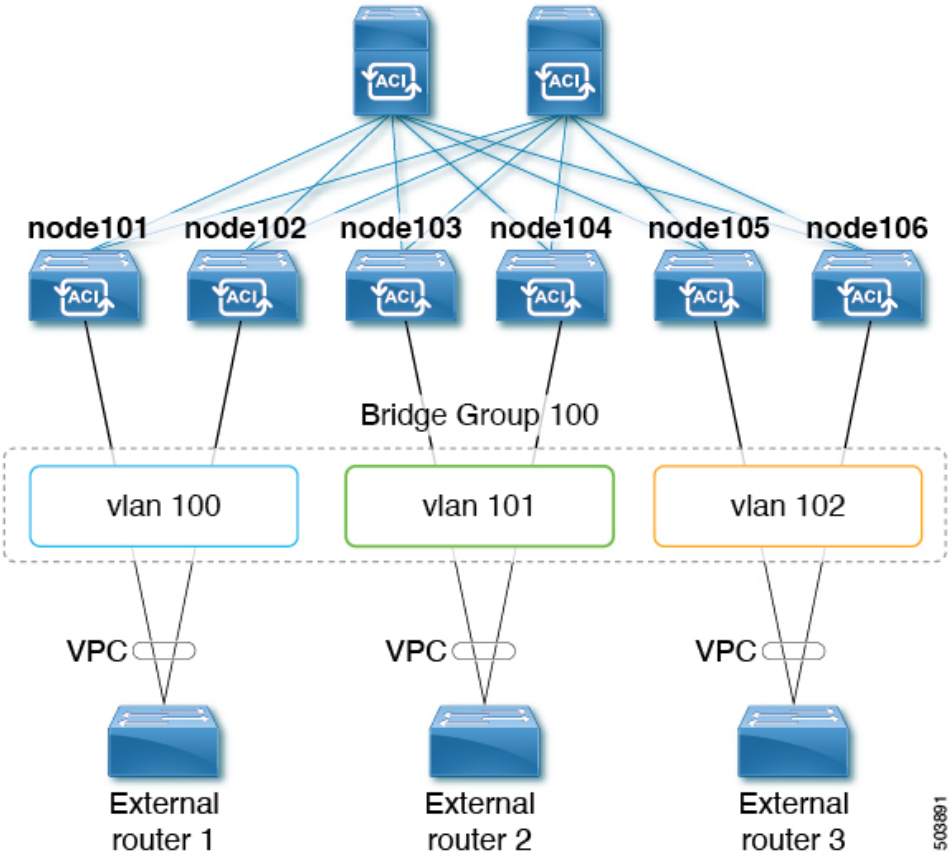
図 *5 :* 異なるカプセル化で外部ブリッジ ドメインに関連付けられた単一の *VNID*（*ACI 5.2(3)* 以降のリリース）。



ACI リリース 6.0(1) の時点で、この機能は物理ドメイン L3Out に対してのみサポートされ、VMM ドメイン L3Out に対してはサポートされません。

複数の SVI を異なるアクセスのカプセル化でグループ化する

次の図は、複数の SVI が異なるアクセス カプセル化でグループ化されている設定を示しています。



この使用ケースでは：

- 次のリーフ スイッチは VPC ペアです。
  - node101 および node102
  - node103 および node104
  - node105 および node106

複数の SVI をレイヤ 2 ブリッジ グループにグループ化する上記の使用例を設定します。

1. VPC ペアごとに 3 つの通常の SVI を作成します。
   - 通常の SVI **svi-100** をリーフ スイッチ node101 および node102 上で作成
   - 通常の SVI **svi-101** リーフ スイッチ node103 および node104 上で作成
   - 通常の SVI **svi-102** リーフ スイッチ node105 および node106 上で作成
2. リーフ スイッチをアクセス カプセル化に構成します。
   - アクセス カプセル化 **VLAN100** を使用してリーフ スイッチ node101 および node102 を構成します。

- アクセス カプセル化 **VLAN101** でリーフ スイッチ node103 および node104 を構成します。
- アクセス カプセル化 **vlan 102** を使用してリーフ スイッチ node105 および node106 を構成します。

3. 単一のレイヤ2ブロードキャスト ドメインの一部として動作するために通常の SVI **svi-100**、**svi-101**、および **svi-102** をグループ化します：
   1. ブリッジ ドメイン プロファイルを作成します。

      ブリッジ ドメイン プロファイルは、新しい MO *l3extBdProfile* で表されます。
   2. ブリッジ ドメイン プロファイルの一意の名前文字列を指定します。
   3. 同じブリッジ ドメイン プロファイルにグループ化する必要がある通常および SVI のそれぞれを関連付けます。

      この関連付けには、次の 2 つの新しい MO を使用できます： *l3extBdProfileCont* および *l3extRsBdProfile*。

注意事項と制約事項

- レイヤ 2 ループは、外部デバイス/ハイパーバイザによってブロックされます。ループを防止するためにスパニングツリープロトコルに依存する外部スイッチでこの機能を使用すると、ループが発生する可能性があります。
- SVI は、外部ブリッジ ドメイン プロファイルの設定後に削除され、再度追加されます。
- 外部ブリッジ ドメイン プロファイルは L3Out スコープです。ノードでは、同じ外部ブリッジ ドメイン プロファイルに 2 つの異なるアクセス カプセル化マッピングを設定することはできません。
- ブリッジ ドメインのグループ化は、カプセル化スコープ **ctx**（APIC GUI の **VRF** オプション）ではサポートされていません。
- 異なる回線カプセル化を持つグループ化された SVI は、共通ノードを共有できません。
- リリース 5.2(3) から SVI による L3Out の複数のカプセル化がサポートされていない以前のリリースにダウングレードする場合、複数のカプセル化や外部ブリッジ ドメイン プロファイルで設定された L3Out で次のアクションが実行されます。
  - 複数のカプセル化サポートに使用される新しいアロケータ（*l3extBdProfileEncapAllocator*）が削除されます。
  - すべての外部ブリッジ ドメイン プロファイル（新しい *l3extBdProfile* MO）が削除されます
  - すべての新しい *l3extBdProfileCont* MO が削除されます
  - すべての新しい *l3extRsBdProfile* MO が削除されます

GUI を使用して SVI で複数の L3Out のカプセル化を構成する

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

その手順は、GUI を使用して SVI 外部カプセル化の範囲の構成 （18 ページ） を参照してください。

ステップ 2 SVI グループ化に使用される外部ブリッジ グループ プロファイルを作成します。

a) **[テナント（Tenants）]** > ***[tenant-name]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[外部ブリッジ グループ プロファイル（External Bridge Group Profiles）]**に移動します。
構成済みの外部ブリッジ グループ プロファイルを示すページが表示されます。

b) **[外部ブリッジ グループ プロファイル（External Bridge Group Profiles）]** を右クリックし、**[外部ブリッジ グループ プロファイルの作成（Create External Bridge Group Profile）]**を選択します。
[外部ブリッジ グループ プロファイルの作成（Create External Bridge Group Profile）] ページが表示されます。

c) 外部ブリッジ グループ プロファイルの名前を入力し、**[送信（Submit）]**をクリックします。
すでに構成されている外部ブリッジ グループ プロファイルを示すページが、新しい外部ブリッジ グループ プロファイルで更新されます。

ステップ 3 通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

a) **[テナント（Tenants）]** > ***[tenant-name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out-name]*** > **[論理ノード プロファイル（Logical Node Profile）]** > ***[log-node-profile-name]*** > **[論理インターフェイス プロファイル（Logical Interface Profile）]** > ***[log-int-profile-name]***に移動します。
この論理インターフェイス プロファイルの **[全般（General）]** ページが表示されます。

b) **SVI** タブをクリックします。
構成済みのスイッチ仮想インターフェイスを示すページが表示されます。

c) 外部ブリッジ ドメイン プロファイルに関連付けるスイッチ仮想インターフェイスをダブルクリックします。
このスイッチ仮想インターフェイスの一般情報が表示されます。

d) **[外部ブリッジ グループ プロファイル（External Bridge Group Profile）]** フィールドで、このスイッチ仮想インターフェイスに関連付ける外部ブリッジ ドメイン プロファイルを選択します。

e) **[送信（Submit）]**をクリックします。

CLI を使用して SVI で複数の L3Out のカプセル化を構成する

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定 を参照してください。

ステップ 2 CLI を使用して APIC にログインし、構成モードとテナント構成モードを開始します。

```
apic1#
apic1# configuration
apic1(config)# tenant <tenant-name>
apic1(config-tenant)#
```

ステップ 3 次のコマンドを入力して、SVI グループ化に使用する外部ブリッジ プロファイルを作成します。

```
apic1(config-tenant)# external-bridge-profile <bridge-profile-name>
apic1(config-tenant-external-bridge-profile)# ?
```

ステップ 4 次のコマンドを入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
apic1(config)# leaf <leaf-ID>
apic1(config-leaf)# interface vlan <vlan-num>
apic1(config-leaf-if)# vrf member tenant <tenant-name> vrf <VRF-name>
apic1(config-leaf-if)# ip address <IP-address>
apic1(config-leaf-if)# external-bridge-profile <bridge-profile-name>
```

REST API を使用した複数の SVI 付き L3Out のカプセル化の設定

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

その手順の REST API を使用して、SVI インターフェイスのカプセル化スコープの設定 を参照してください。

ステップ 2 次の例のような投稿を入力して、SVI グループ化に使用する外部ブリッジ プロファイルを作成します。

```
<fvTenant name="t1" dn="uni/tn-t1" >
    <l3extBdProfile name="bd100" status=""/>
</fvTenant>
```

ステップ 3 次の例のように投稿を入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
<fvTenant name="t1">
    <l3extOut name="l1">
        <l3extLNodeP name="n1">
            <l3extLIfP name="i1">
                <l3extRsPathL3OutAtt encap="vlan-108"
tDn="topology/pod-1/paths-108/pathep-[eth1/10]"                    ifInstT="ext-svi">
                    <l3extBdProfileCont>
                        <l3extRsBdProfile tDn="uni/tn-t1/bdprofile-bd100" status=""/
      ></l3extBdProfileCont>
                </l3extRsPathL3OutAtt>
            </l3extLIfP>
        </l3extLNodeP>
```

```
    </l3extOut>
</fvTenant>
```

ステップ 4 フローティング ノードの個別のカプセル化を指定するには、次の例のような投稿を入力します。

```
<fvTenant name="t1">
    <l3extOut name="l1">
        <l3extLNodeP name="n1">
            <l3extLIfP name="i1">
                <l3extVirtualLIfP addr="10.1.0.1/24"                    encap="vlan-100"
              nodeDn="topology/pod-1/node-101"                        ifInstT="ext-svi">
                    <l3extRsDynPathAtt floatingAddr="10.1.0.100/24"
encap="vlan-104"                          tDn="uni/phys-phyDom"/>
                </l3extVirtualLIfP>
            </l3extLIfP>
    </l3extOut>
</fvTenant>
```

SVI 自動状態

SVI 自動状態について

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できます。APIC リリース 3.0(x) ではサポートされていません。

スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。SVIは、物理ポート、直接ポートチャネル、仮想ポートチャネルのメンバーを有することができます。SVI論理インターフェイスはVLANに関連付けられ、VLAN ポート メンバーシップを有します。

SVI の状態はメンバーに依存しません。Cisco APIC の SVI のデフォルトの自動状態動作は、自動状態の値が無効になっているときに最新の状態になっていることを意味します。これは、インターフェイスが対応するVLANで動作していない場合、SVIがアクティブであることを意味します。

SVI 自動状態の値を有効に変更する場合、関連する VLAN のポート メンバーに依存します。VLANインターフェイスがVLANで複数のポートを有する場合、SVIはVLANのすべてのポートがダウンするとダウン状態になります。

表 *2: SVI* 自動状態

SVI 自動状態	SVI 状態の説明
ディセーブル	インターフェイスが対応する VLAN で動作していない場合、SVI がアップ状態であることを意味します。 無効がデフォルトの SVI 自動状態の値です。

SVI 自動状態	SVI 状態の説明
有効	SVI は、関連付けられている VLAN のポート メンバによって異なります。VLAN インターフェイスに複数のポートを含む場合、SVI は VLAN のすべてのポートがダウンするとダウン状態になります。

SVI 自動状態の動作のガイドラインと制限事項

次のガイドラインをお読みください。

- SVI の自動状態の動作を有効化または無効化にすると、SVI あたりの自動状態の動作を設定します。これらはグローバル コマンドではありません。

GUI を使用した SVI 自動状態の構成

始める前に

- テナントと VRF が構成されています。
- L3Out が構成されており、L3Out の論理ノードプロファイルと論理インターフェイス プロファイルが構成されています。

手順

ステップ 1 メニュー バーで、 > **[テナント（Tenants）]** > ***[tenant-name]***をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[LogicalNodeProfile_name]*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]**をクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[論理インターフェイス プロファイル（Logical Interface Profile）]**を展開し、適切な論理的なインターフェイス プロファイルをクリックします。

ステップ 4 作業ペインで、**SVI** タブをクリックし、+ サインをクリックして **SVI** ダイアログ ボックスを表示します。

ステップ 5 追加の SVI を追加するには、**SVI** ダイアログボックスで、次の操作を実行します：

a) **[パスタイプ（Path Type）]** フィールドで、適切なパス タイプを選択します。

b) **[パス（Path）]** フィールドで、ドロップダウンリストから適切な物理インターフェイスを選択します。

c) **[カプセル化（Encap）]** フィールドで、適切な値を選択します。

d) **[自動状態（Auto State）]** フィールドで、**[作業（Work）]** ペインの SVI を選択し、自動状態の値を表示または変更します。

デフォルト値は、**[無効化（Disabled）]**です。

（注）

既存 SVI の自動状態の値を確認または変更するには、適切な SVI を選択して、値を確認または変更します。

Cisco フローティング L3Out について

以降では、[Cisco Application Policy Infrastructure Controller]（[APIC]）リリース 4.2（1）以降では、外部ネットワークデバイスに接続するための複数のレイヤ3外部ネットワーク接続（L3Out）論理インターフェイスパスを指定する必要がなくなりました。

このフローティングL3Out機能を使用すると、論理インターフェイスを指定せずにL3Outを設定できます。この機能により、仮想マシン（特定の仮想ネットワーク機能を実行する）がホスト間を移動する際に、ルーティングを維持するために複数のL3Out論理インターフェイスを設定する必要がなくなります。フローティングL3Outは、VMware vSphere分散スイッチ（VDS）を持つ VMM ドメインでサポートされています。

[Cisco APIC] リリース 5.0（1）以降のリリースでは、物理ドメインがサポートされています。これは、同じ単純化された構成を物理ルータの展開にも使用できることを意味します。

詳細については、次の資料を参照してください。 *[フローティング L3Out を使用した外部ネットワーク接続の簡素化（Using Floating L3Out to Simplify Outside Network Connections）]* ナレッジ ベースの記事：

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Floating-L3Out.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。