SD-Access と ACI 統合

Cisco SD-Access と Cisco ACI の統合

（注） Cisco Nexus Dashboard と Cisco DNAC の統合により、Nexus とキャンパス SD Accessファブリックの展開全体で、ネットワーク接続のサブセットとマクロセグメンテーション シナリオの自動化が可能になります。この統合は、限られた可用性の下にあります。詳細についてはシスコの担当者にお問い合わせください。

Cisco Software-Defined Access（SD Access または SDA）は、Cisco Digital Network Architecture（DNA）内のソリューションであり、Cisco のインテントベース ネットワーク（IBN）フレームワークを実装するキャンパスおよびブランチ アーキテクチャを定義します。Cisco SD-Access は、セキュリティ、自動化、およびアシュアランスによってビジネスニーズを満たす、統一されたポリシー ベースの有線およびワイヤレスネットワーク ファブリックを定義します。Cisco Identity Services Engine（ISE）と組み合わせた、Cisco Digital Network Architecture Controller（DNAC）は、Cisco SD-Access ファブリックの自動化と管理の統合ポイントです。

Cisco Nexus Dashboard Orchestrator（NDO）のリリース 3.7(1) では、Cisco SD-Access および Cisco ACI 統合のサポートが追加されています。SD Access および ACI 統合の目的は、キャンパスおよびブランチ ネットワークをデータセンター ネットワークにセキュアに接続することです。リリース 3.7(1) では、NDO は次の機能を実行できます。

- 両方のドメインからネットワークとリソースの情報を収集する
- ACI 側で VRF-Lite ドメイン間接続を自動的に設定する
- SD Access ボーダーノードに接続されているネクスト ホップ デバイスの構成を提供します。
- クロスドメインの可視性を提供する

マクロセグメンテーション

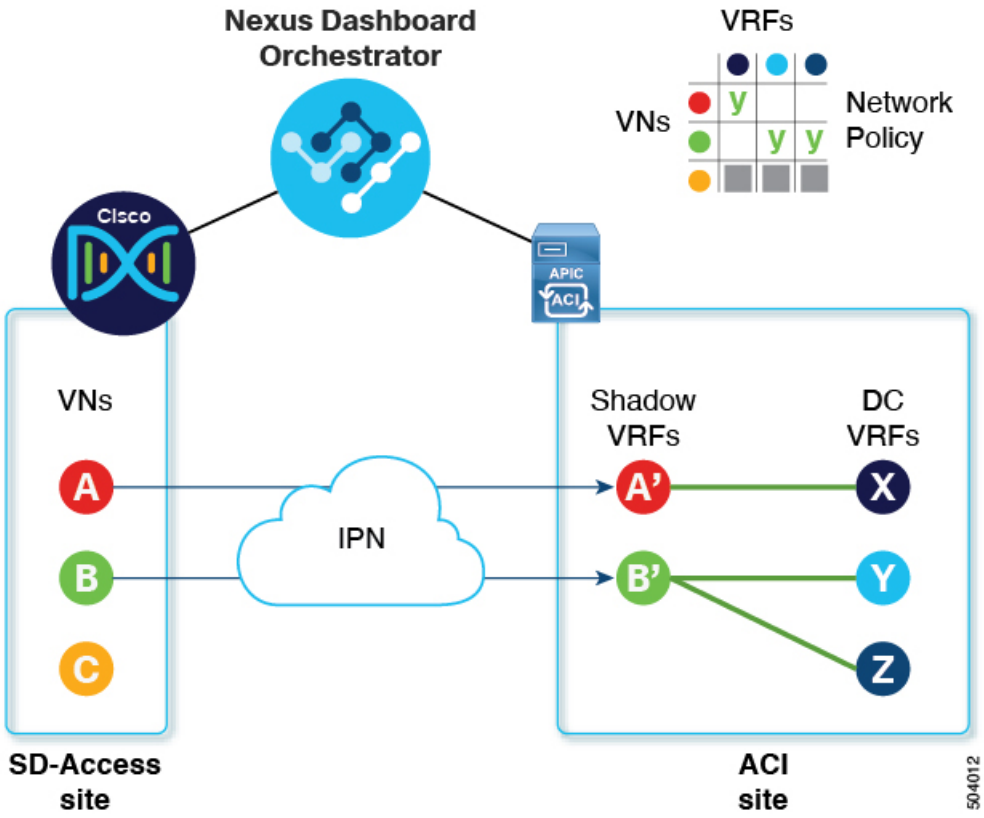
Cisco Nexus Dashboard Orchestrator（NDO）の統合機能により、ACI ドメインとドメイン間のネットワーク要素のマクロセグメンテーションが可能になります。Cisco SD-AccessCisco ACISD Access

ACI ドメインでは、EPG、サブネット、VLAN などのエンティティは、仮想ルーティングおよび転送インスタンス（VRF）の一部としてグループ化されます。VRF が外部通信を必要とする場合、VRF は ACI ボーダー リーフ（BL）の IP インターフェイス（L3Out）に関連付けられます。ドメインでは、ユーザー、サブネット、IP プールなどのエンティティを仮想ネットワーク（VN）としてグループ化できます。SD AccessVN が外部通信を必要とする場合、VN は IP ハンドオフのためにボーダーノード（BN）インターフェイスに関連付けられます。SD Access2 つのドメイン、ACI のボーダー インターフェイスは、IP ネットワーク（IPN）を介して物理的に接続できますが、この基本的な接続は VRF と VN 間の接続を提供しません。SD AccessCisco Nexus Dashboard Orchestrator Cisco SD-Access および Cisco ACI インテグレーションにより、管理者は、VRF を VN にマッピング（または「ステッチ」）するポリシーを作成できます。

マクロセグメンテーション ワークフロー

一般的なCisco SD-Access および Cisco ACI インテグレーション ワークフローは、次の図を参照する次の手順で構成されます。

図 *1 : SD-Access-to-ACI* 統合のための *NDO* を使用したマクロセグメンテーション



- 既存の SD Access サイトでは、Cisco Digital Network Architecture Controller（DNAC）管理者がキャンパス ファブリックを構成しており、一部のエンティティはデータセンターへのアクセスなどの外部アクセスを必要とします。DNAC 管理者は、次のタスクを実行します。
  - 作成済みの仮想ネットワーク（VN）
  - それらの VN に関連付けられた IP アドレスプール
  - 構成された L3 ボーダーノードおよび関連するインターフェイス
  - 作成済み IP（レイヤ 3）ハンドオフ トランジットネットワーク
  - 外部接続を必要とする VN 用に設定されたレイヤ 3 ハンドオフ

  これらのタスクは通常の DNAC 管理タスクであり、インテグレーションのために特別な変更は行われていないことに注意してください。Cisco SD-AccessCisco ACI

- NDO オペレーターは、DNAC ログイン情報を使用して、DNAC にログインして導入準備します。

  オンボーディング プロセスでは、NDO は自動的に DNAC の REST API にアクセスして、サイト、VN、およびボーダーノード デバイスをクエリします。これらのエンティティを検出すると、NDO はどの VN が外部接続（L3 ハンドオフ）用に構成され、どのボーダー

ノードであるかを学習し、それらのサブネットを学習します。Cisco SD-Access図 1 : SD-Access-to-ACI 統合のための NDO を使用したマクロセグメンテーション （3 ページ）に示す例では、VN A と B は L3 ハンドオフ用に設定されており、これらの VN は ACI サイトに拡張するために使用できます。VN C は L3 ハンドオフ用に構成されておらず、ACI サイトで使用できません。

NDO は、SD Access ファブリック内の進行中の構成変更について DNAC に定期的にクエリを実行し続けます。

- NDO オペレーターは、1 つ以上の ACI サイトと 1 つ以上の SD Access サイト間の接続を構成します。これには、ACI サイトのボーダー リーフスイッチとインターフェイス、およびボーダー リーフ インターフェイスでの VRF-Lite 構成に使用される VLAN と IP プールの指定が含まれます。直接接続されたインターフェイス（IPN なし）の場合、VRF-Lite 構成は、SDA ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされた構成から取得され、VLAN と IP アドレスはこれらのプールから取得されません。

  NDO は、拡張 SD Access VN のネクストホップ デバイス構成を生成して表示します。この構成は、必要に応じて IPN デバイスに手動で適用できます。NDO は IPN デバイスをプロビジョニングしません。

- NDO オペレーターは VN をデータセンターに拡張し、VN を ACI ドメイン内の VRF に接続できるようにします。

  VN を拡張すると、ACI ドメイン上の VN を表す VN の内部表現（ミラーリングされた「シャドウ VRF」）が作成されます。図 1 の例では、シャドウ VRF A' と B' が ACI サイトに自動的に作成され、拡張 SD Access VN A と B を表します。これらのシャドウ VRF は、SD Access ドメインとの接続を必要とする ACI ドメイン内のすべてのサイトとポッドに拡張されます。NDO は、これらのシャドウ VRF が構成されているスキーマとテンプレートを自動的に作成します。自動作成されたスキーマとテンプレートは NDO に表示されますが、読み取り専用です。テンプレートは「共通」テナントに関連付けられており、「SDA 接続」が有効なすべてのサイトに関連付けられています。

- NDO オペレーターは、拡張 SD Access VN をデータセンター VRF または VN がアクセスする必要のある VRF にマッピングするネットワーク ポリシーを作成します。このアクションは、「VRF スティッチング」とも呼ばれます。データセンターの VRF は、さまざまな「アプリ テナント」の一部にすることができます。これは、設計によるこの統合により、VRF 間接続（通常は「共有サービス」と呼ばれる機能）を確立できることを意味します。

  図 1 の例では、示されているネットワーク ポリシーは、拡張 SD Access VN A（VRF A' として拡張）をデータセンター VRF X に、VN B（VRF B' として拡張）をデータセンター VRF Y および Z にステッチしています。

  このマッピングの結果として、すべてのトラフィックを許可するセキュリティポリシー関係が、拡張 SD Access VN に関連付けられた L3Out の外部 EPG とデータセンター VRF を表す vzAny 論理オブジェクトとの間に自動的に確立されます。この契約の適用により、拡張 SD Access VN のすべてのサブネットと、VRF 間で漏洩するように明示的に構成されたデータセンター VRF のすべてのサブネットとの間で無料の接続が可能になります。

Cisco SD-Access およびCisco ACI インテグレーション ガイドライン

- ACI サイトと SD Access サイトは、外部 IP ネットワーク（IPN）を介して間接的に接続することも、ACI ボーダー リーフから SD Access ボーダーノードへのバックツーバック接続で直接接続することもできます。
  - サイトが直接接続されている場合、2 つのドメイン間の接続は、コントロールプレーンとデータプレーンの両方を含め、自動的に構成されます。
  - サイトが IPN を使用して接続されている場合、IPN デバイスは VRF Lite をサポートする必要があります。NDO および DNAC は IPN デバイスをプロビジョニングしませんが、NDO は、ACI ボーダー リーフおよび SD Access ボーダーノードに直接接続されている IPN デバイスに適用できるサンプル構成を提供します。
- いずれかのドメインに複数のサイトが存在する場合は、次のガイドラインに注意してください。
  - SD Access サイトは別の SD Access サイト（SDA トランジット）を使用して ACI サイトに接続できます。
  - SD Access（キャンパス）ドメインに複数のサイトが存在する場合、各キャンパス サイトはデータセンター ドメインに直接接続するか（ダイレクト ピアリング）、汎用 IP ネットワーク（IPN）などの中間ネットワークを介して、または別のキャンパス サイトを介して（間接ピアリング）接続できます。
  - マルチサイト展開では、SD Access（キャンパス）ドメインとの直接または間接接続を必要とする各 ACI ファブリックは、ローカル L3Out 接続を展開する必要があります。ACI ファブリックがマルチポッドファブリックの場合、L3Out 接続は、同じファブリックの一部であるポッドまたはポッドのサブセットにのみ展開できます。
- SD Access と ACI 統合の拡張性 （6 ページ） で説明されている制限内で、VN から VRF への M:N マッピングがサポートされています。
- で説明されている制限内で、サイトから ACI サイトへの M:N マッピングがサポートされています。SD AccessSD Access と ACI 統合の拡張性 （6 ページ）
- DNAC から、NDO はすべての SD Access（キャンパス）VN とそのサブネットについて学習します。VN が ACI サイトに拡張されると、NDO は、その拡張された VN のすべてのサブネットが ACI 境界リーフから到達可能であると想定します。NDO は、ACI ボーダー リーフにこれらのサブネットが存在するかどうかを定期的に確認します。拡張 VN の [インテグレーション（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）] テーブルの [ステータス（Status）] 列で、NDO はまだ到達できないサブネットを報告します。

- デフォルトでは、拡張 VN が DC VRF にマッピングされている場合、ACI サイトは通過ルートを VN にアドバタイズしません。NDO 管理者は、どの ACI サブネットが VN のシャドウ VRF にリークされるかを次のように制御します。
  - ACI VRF の内部にある BD サブネットは、サブネットが「VRF 間で共有」で設定されている場合にのみリークされます。

（注） SD Access VN が複数の ACI VRF にマッピングされている場合、マッピングされたすべての ACI VRF で重複しないプレフィックスのみを「VRF 間で共有」として設定する必要があります。

  - ACI VRF で設定された L3Out から学習した外部サブネットは、サブネットが「共有ルート制御」で設定されていて、トランジット ルーティングが有効になっている場合にのみリークされます。

詳細については、トランジット ルーティングの設定 （17 ページ）を参照してください。

- SD Access サイトは、ACI サイトへのインターネット接続を提供できません。
- IPv6 接続の自動化はサポートされていません。
- マルチキャスト トラフィックはドメイン間でサポートされていません。

SD Access と ACI 統合の拡張性

- NDO および ACI 統合にオンボーディングできる DNAC は 1 つだけです。SD Access
- 単一の DNAC で管理されている場合、複数の（キャンパス）サイトがサポートされます。SD Access
- ピアリングでは、最大 2 つの ACI サイトがサポートされます。SD Access各 ACI サイトは、単一のポッドファブリックまたはマルチポッドファブリックにすることができます。
- 仮想ネットワーク（VN）は、最大 10 個の ACI VRF にマッピングできます。
- ドメインから最大 32 個の仮想ネットワーク（VN）を ACI ドメインに拡張できます。SD Access

ソフトウェアの互換性

マクロセグメンテーションと ACI 統合をサポートする最小ソフトウェア バージョンを次の表に示します。SD Access

製品	サポート対象の製品バージョン
NDO	3.7 以降のリリース
ACI	4.2 以降のリリース
DNAC	2.3.3 以降のリリース

DNA センターのオンボーディング

このセクションでは、Cisco Templates Nexus Dashboard Orchestrator（NDO）を構成して DNA センター（DNAC）にログインする方法について説明します。サインイン後、NDO は SD Access ドメインと ACI ドメイン間のネットワーク接続を作成するために必要な SD Access サイト構成情報をインポートできます。

ステップ 1 NDO にログインします。

ステップ 2 左のナビゲーション ペインで、**[管理（Admin）] > [統合（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[DNAC の追加（Add DNAC）]** をクリックして DNA センターをオンボードします。

[**DNAC の追加（Add DNAC**）] ダイアログボックスが開きます。

ステップ 4 [**DNAC の追加（Add DNAC**）] ダイアログボックスで、次の手順を実行します。

a) DNA センターの [**名前（Name**）] を入力します。
b) DNA センターの URL または IP アドレスをデバイス IP として入力します。
c) DNA センターにサインインするための **[ユーザー名（Usesrname**）] 資格情報を入力します。

読み取り専用アクセスで十分です。

d) DNA センターにサインインするための **[パスワード（Password**）] 資格情報を入力します。
e) **[Confirm Password（パスワードの確認）]** に、もう一度パスワードを入力します。
f) **[追加（Add）]** をクリックします。

NDO は、REST API を介して DNAC に自動的にサインインし、DNAC によって制御される SD Access ドメイン内の仮想ネットワーク（VN）およびボーダーノード デバイスの構成を照会します。

次のタスク

- ACI サイトからサイトまたは IPN への接続を構成します。SD Access
- DNAC のドメインの VN と ACI ドメインの VRF 間の通信を許可するネットワーク ポリシーを作成します。SD Access

SD Access ドメインへの接続の構成

このセクションでは、ACI 統合のために Cisco SD-Access の NDO で実行されるインフラストラクチャ レベルの構成について説明します。ACI ファブリックごとに、Cisco SD-Access ドメインへの接続を提供するボーダー リーフ ノードとそれらに関連付けられたインターフェイスを選択する必要があります。

始める前に

Cisco DNA Center をオンボードする必要があります。

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

ステップ 2 左のナビゲーション ペインで、**[管理（Admin）] > [統合（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[概要（Overview）]** タブをクリックします。

DNA Center のダッシュボードが表示されます。

ステップ 4 [DNAC の詳細（DNAC Details）] ボックスの右側で、[接続の構成（Configuring Connectivity）] のリンクをクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 5 左側のナビゲーションペインの [サイト（Sites）] で、接続する ACI サイトを選択します。

[サイト接続（Site Connectivity）] ペインが右側に表示されます。

ステップ 6 [サイト接続（Site Connectivity）] ウィンドウで、[SDA 接続（SDA Connectivity）] コントロールまで下にスクロールし、[有効（Enabled）] に設定します。

[SDA 接続（SDA Connectivity）] コントロールの下にいくつかのフィールドが表示されます。以下のサブステップで設定を構成します。

a) **[外部ルーテッド ドメイン（External Routed Domain）]** ドロップダウン リストから、接続する外部ルーテッド ドメイン（L3 ドメイン）を選択します。

このルーテッド ドメインは、APIC ですでに定義されている必要があります。

b) **[VLAN プール（VLAN Pool）]** フィールドに、VLAN の番号の範囲を入力します。

このプールの VLAN 番号は、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。VLAN プールは、前の手順で選択した外部ルーテッド ドメインに関連付けられた VLAN プールと同じか、そのサブセットである必要があります。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、VLAN ID はこのプールから割り当てられません。代わりに、VLAN ID は、SD Access ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

c) [VRF Lite IP プール範囲（VRF Lite IP Pool Ranges）] で、[VRF Lite IP プール範囲を追加（Add VRF Lite IP Pool Range）] の横にある [+] 記号をクリックし、[IP アドレス（IP Address）] フィールドに IP サブネットを入力します。

このサブネットの IP アドレスは、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、これらのプールは使用されません。この場合、サブインターフェイスの IP アドレスは、SD Access ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

ステップ 7 ACI サイトのポッドが表示されている中央のペインで、サイトに接続するポッドの下にある [リーフ ノードの追加（Add Leaf Node）] をクリックします。SD Access

[リーフの選択（Select a Leaf）] ペインが右側に表示されます。以下のサブステップで設定を構成します。

a) **[リーフの選択（Select a Leaf）]** ペインの **[リーフノード（Leaf Node）]** ドロップダウン リストから、SD Access ドメインに接続するボーダー リーフ スイッチを選択します。
b) **[ルータ ID（Router ID）]** フィールドに、ボーダーリーフ スイッチ ルータ ID を入力します。
c) [インターフェース（Interfaces）] で、[インターフェースの追加（Add Interface）] の横にある [+] 記号をクリックします。

[Add Interface] ダイアログボックスが表示されます。

d) **[インターフェイス ID（Interface ID）]** を入力します。
e) [インターフェイス タイプ（Interface Type）] ドロップダウンリストから [サブインターフェイス（Sub-Interface）] または [SVI] を選択します。
f) **[リモート自律システム番号（Remote Autonomous System Number）]** を入力します。

ACI から SD Access への接続が IPN を使用する場合、この番号は IPN の ASN と一致する必要があります。

ACI から SD Access への接続が IPN なしでバックツーバックである場合、この番号は SD Access ボーダーノードの ASN と一致する必要があります。

g) [保存（Save）] をクリックします。

ステップ 8 [ファブリック接続インフラ（Fabric Connectivity Infra）] ページの上部のバーで、[展開（Deploy）] をクリックします。

この時点では、構成はまだ APIC にプッシュされていません。最初の VN が拡張されると、SD Access 接続が自動的に構成されます。

ACI 統合への SD Access のステータスの表示

[インテグレーション（Integrations）]>[DNAC] メニューには、統合ステータスに関する詳細が表示され、使用可能な仮想ネットワーク（VN）のインベントリが提供されます。

[概要（Overview）] タブ

[概要（Overview）] タブは、次の情報ウィンドウを表示します。

- [DNAC 詳細（DNAC Details）]：接続されている DNAC の全体的なステータス、IP アドレス、およびバージョンを表示します。このウィンドウには、[接続の構成（Configure Connectivity）] へのリンクも含まれています。
- 次のリソースの概要グラフィック ダッシュボード：

- [DNAC 可能なサイト（DNAC Enabled Sites）]：DNAC によって管理されているサイトの数とタイプ。SD Accessサポートされているサイト タイプは、オンプレミス、AWS、および NDFC です。
- [仮想ネットワーク（Virtual Networks）]：使用可能な VN の数、および拡張または拡張されていない数。
- [DC VRF]：共有に使用できるデータセンター VRF の数、およびそれらがマッピングされているかどうか。

[仮想ネットワーク（Virtual Networks）] タブ

[仮想ネットワーク（Virtual Networks）] タブをクリックして、VN に関する詳細を表示します。

ページの上部のウィンドウには、[概要（Overview）] タブからの概要グラフィック情報が繰り返されます。

このページの [仮想ネットワーク（Virtual Networks）] ウィンドウには、ボーダー ノードでの IP ハンドオフ用に DNAC によって構成された仮想ネットワーク（VN）が一覧表示されます。SD AccessVN のテーブルには、VN ごとに次の情報が表示されます。

- [ステータス（Status）]：VN の現在の統合ステータスと、ステータスの重大度を示す色分けされたアイコン。状態を次の表に示します。

ステータス	アイコンの色（重大度）	説明
検出済	緑色（正常）	VN は SDA ボーダー ノードで検出されます。
処理中	グレー （情報）	構成変更後の VN の最新ステータスを読み取ります。これは一時的な状態です。 **ヒント** ページの右上隅にある [更新] アイコンをクリックして、ステータスの即時ポーリングを強制することができます。
成功	緑色（正常）	VN は正常に拡張されました。
[BGPSessionIssues]	黄色（警告）	すべてのインターフェイスで BGP セッションが確立されているわけではありません。詳細については、各 DC ボーダー リーフの状態を確認してください。
[RouteLeakPartial]	黄色（警告）	VN サブネットは、DC ボーダー リーフ ノードに部分的に伝達されます。詳細については、各 DC ボーダー リーフの状態を確認してください。
[RouteLeakNone]	赤（失敗）	VN サブネットはまだ DC ボーダー リーフ ノードに伝達されていません。VN テーブルで [DC サイト（DC Sites）] をクリックして、DC ボーダー リーフ インターフェイスに問題がないか確認します。

ステータス	アイコンの色（重大度）	説明
[MappedVRFConfigFailure]	赤（失敗）	マッピングされた VRF で設定が失敗しました。マッピングを再試行します。
[DCSiteConfigFailure]	赤（失敗）	DC サイトで VN 拡張が失敗しました。VN の拡張を解除して、再度拡張します。

VN のステータス アイコンをクリックして、警告やエラーのトラブルシューティングに役立つ追加の詳細を含むサイドバーを表示します。

- [名前（Name）]：DNAC 管理者によって VN に割り当てられた名前。
- [拡張済み（Extended）]：VN が拡張されているかどうかを示します。
- [DC マップ済みの VRF（DC Mapped VRFs）]：VN がマップされるデータセンター VRF の数。この番号をクリックしてサイドバーを開き、マッピングされたデータセンター VRF の関連スキーマ、テンプレート、およびテナントを表示します。
- [DC サイト（DC Site）]：VN がマップされているデータセンター サイトの数。この番号をクリックしてサイドバーを開き、ボーダー リーフ インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、データセンター サイトの詳細を表示します。

ヒント　IPN 接続のボーダー リーフ インターフェイスの場合、サイドバーの [ピア デバイスの構成（Peer Device Configuration）] で、[詳細の表示（Show Details）] をクリックして、このサイトに接続されている IPN デバイスの構成例を表示します。

- [キャンパス サイト（Campus Sites）]：この VN に関連付けられているキャンパス サイトの数。この番号をクリックしてサイドバーを開き、ボーダー ノード インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、キャンパス サイトの詳細を表示します。

ヒント　IPN 接続のボーダー ノード インターフェイスの場合、サイドバーの [ピア デバイスの構成（Peer Device Configuration）] で、[詳細の表示（Show Details）] をクリックして、このサイトに接続されている IPN デバイスの構成例を表示します。

- […（アクション アイコン）（… (actions icon)）]：アイコンをクリックして、この VN のアクションにアクセスします。

  使用可能なアクションは、VN の現在のステータスによって異なりますが、次のものが含まれる場合があります。

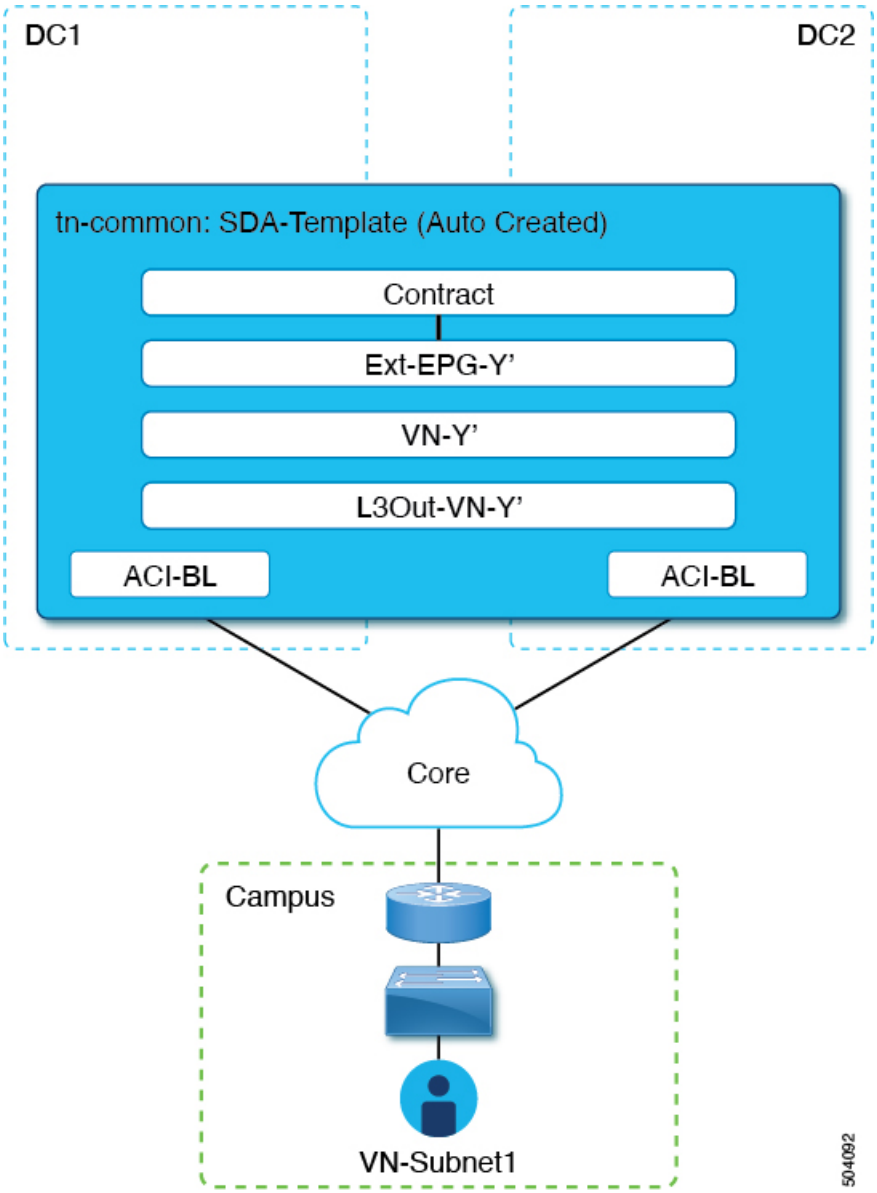
- VN の拡張 / 拡張解除
- DC VRF のマッピング / マッピング解除
- トランジット ルートの有効化 / 無効化

キャンパス VN をデータセンター VRF にマッピングすると、[仮想ネットワーク（Virtual Networks）] ページの [関連付けテンプレート（Associated Templates）] ウィンドウが表示されます。

仮想ネットワークの拡張

このセクションでは、SD Access（キャンパス）VN を ACI（データセンター）ファブリックに拡張する方法について説明します。このアクションにより、DC 側のキャンパス VN のミラーリングされたイメージを表す VRF（および 図 2 : VN の拡張 （13 ページ） に示す他の関連する構成オブジェクト）が作成されます。作成されたオブジェクトは、「共通」テナントに関連付けられた自動生成テンプレートで定義されます。

図 *2 : VN* の拡張



始める前に

- DNA センター（DNAC）をオンボーディングしておく必要があります。
- ACI サイト レベルでドメインへの接続を構成しておく必要があります。SD Access

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

ステップ 2 左のナビゲーション ペインで、**[管理（Admin）] > [統合（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

仮想ネットワーク（VN）のテーブルが表示され、ボーダーノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。SD Access

ステップ 4 拡張する VN の行で、アクション メニュー（**[...]**）をクリックし、**[拡張（Extend）]** を選択します。

ダイアログ ボックスが開き、VN が拡張される ACI サイトとインターフェイスが表示されます。この情報は、SD Access ドメインへの接続の構成 （7 ページ）の構成設定を反映しています。

VN の拡張を後で取り消す場合は、アクション メニュー（**[...]**）をクリックし、[拡張解除（Unextend）] を選択します。

ステップ 5 ダイアログボックスで、**[はい（Yes）]** をクリックします。

VN は、接続が有効になっているすべての ACI サイトに拡張されますが、まだどの ACI VRF にもマッピングされていません。SD Access

ステップ 6

次のタスク

ACI ボーダー リーフ スイッチ インターフェイスの BGP ピアリング ステータスを確認します。

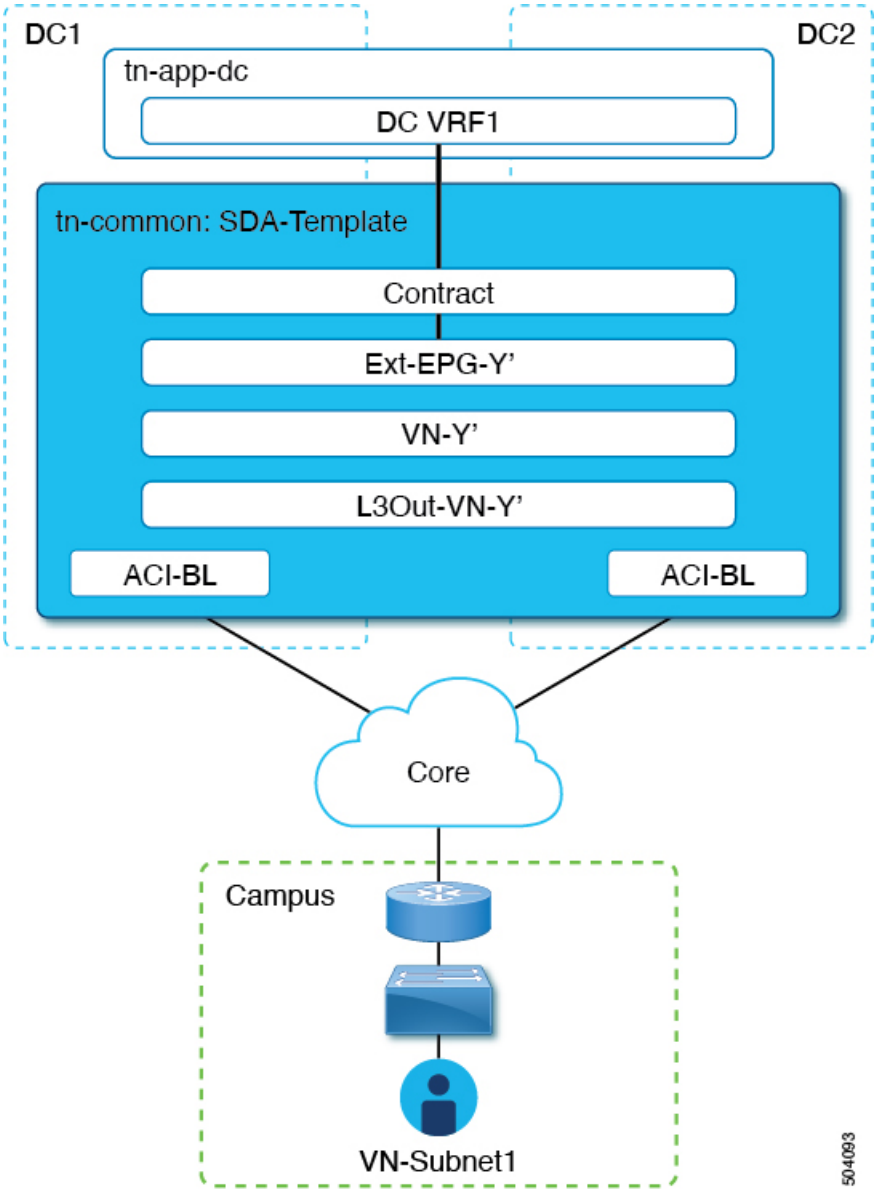
- SD Access ボーダーノードと ACI ボーダー リーフが直接（バックツーバック）接続されている場合は、キャンパス VN を拡張したため、これらのデバイス間で BGP セッションが確立されていることを確認します。**[管理（Admin）] > [統合（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）]** で、**[DC サイト（DC Sites）]** 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ スイッチ インターフェイスの詳細を表示します。ボーダー リーフ スイッチ インターフェイスの BGP ピアリング ステータスが「**Up**」を示していることを確認します。
- IPN がドメイン間に展開されている場合は、構成サンプルを取得して、SD Access ボーダーノードおよび ACI ボーダー リーフに直接接続されているネクストホップ デバイスの構成を支援します。**[管理（Admin）] > [統合（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）]** で、**[DC サイト（DC Sites）]** 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ スイッチ インターフェイスの詳細を表示します。IPN 接続されたボーダー リーフ スイッチインターフェイスの場合は、[ピアリングデバイス構成（Peering Device Configuration）] の横にある [詳細を表示（Show Details）] リンクをクリックして、サンプルの IPN デバイス構成を表示します。IPN デバイスを構成したら、ボーダー リーフ スイッチインターフェイスの BGP ピアリング ステータスが「**Up**」を示していることを確認します。

VN の VRF へのマッピングまたはマッピング解除 （15 ページ） で説明されているように、拡張 VN を 1 つ以上の ACI VRF にマッピングします。

VN の VRF へのマッピングまたはマッピング解除

このセクションでは、仮想ネットワーク（VN）を ACI ファブリック内の 1 つ以上のデータセンター（DC）VRF にマッピング（「ステッチ」）する方法について説明します。図 3 : VRF へのマッピング（15ページ）に示すように、VRF へのマッピングにより、DC VRF（「vzAny」オブジェクトによって表される）と「共通」テナントで以前にプロビジョニングされた外部 EPG との間の契約関係が確立されます。

図 *3 : VRF* へのマッピング



始める前に

VN を ACI サイトに拡張しておく必要があります。

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

ステップ 2 左のナビゲーション ペインで、**[管理（Admin）] > [統合（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

仮想ネットワーク（VN）のテーブルが表示され、ボーダーノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。SD Access

ステップ 4 マッピングする VN の行で、アクション メニュー（[...]）をクリックし、[DC VRF のマッピング / マッピング解除（Map/Un-Map DC VRFs）] を選択します。

[DC VRF のマップ/マップ解除（Map/Un-Map DC VRFs）] ダイアログ ボックスが開きます。

ステップ 5 [DC VRF のマップ / マップ解除（Map/Un-Map DC VRFs）] ダイアログボックスで、[DC VRF のマップの追加（Add Mapped DC VRF）] の横にある [+] アイコンをクリックします。

ステップ 6 VRF のドロップダウンリストから VRF を選択します。

選択した VRF がテーブルに追加され、VRF のテンプレートも表示されます。後の手順で必要になるため、テンプレート名を書き留めておいてください。

VN を追加の VRF にマッピングする場合は、[+] アイコンを再度クリックして、ドロップダウンリストから追加の VRF を選択します。

既存のマッピングを削除して、DC VRF のマッピングを解除することもできます。DC VRF のマッピングを解除するには、VRF の行にあるごみ箱アイコンをクリックします。

ステップ 7 [保存（Save）] をクリックし、VN ステータスが「成功」に変わるまで待ちます。

（注） この時点で、VN ステータスが「成功」を示していても、拡張 VN と DC VRF 間のデータ接続はまだ確立されていません。マッピング操作により、マッピングされた VRF に関連付けられたテンプレートが変更されました。接続が確立される前に、テンプレートを再展開する必要があります。VN テーブルの下の **[関連付けられたテンプレート（Associated Templates）]** テーブルに、マッピングされた VRF に関連付けられたテンプレートが表示されます。

ステップ 8 **[管理（Admin）] > [統合（Integrations）] > > [DNAC] > [仮想ネットワーク（Virtual Networks）]** タブにある **[関連付けられたテンプレート（Associated Templates）]** テーブルで、マッピングされた VRF に関連付けられているテンプレートのリンクをクリックします。

スキーマとテンプレート ページが開きます。

ステップ 9 スキーマとテンプレートのページで、[サイトに配置（Deploy to sites）] をクリックします。

ステップ 10 テンプレートのレビューと承認（変更管理）が有効になっている場合は、変更管理ワークフローに従ってテンプレートを再展開します。それ以外の場合、**[展開（Deploy）]** をクリックして、テンプレートを再展開します。

次のタスク

（注） DC VRF のマッピングを解除した場合、[関連付けられたテンプレート（Associated Templates）] テーブルにテンプレートは表示されません。ただし、**[構成（Configure）] > [テナント テンプレート（Tenanat Template）] > [アプリケーション（Applications）]** に移動し、[スキーマ（Schemas）] を選択して、関連付けられているテンプレートを再展開して、vzAny 構成を削除します。それ以外の場合、データ プレーン通信は有効のままです。

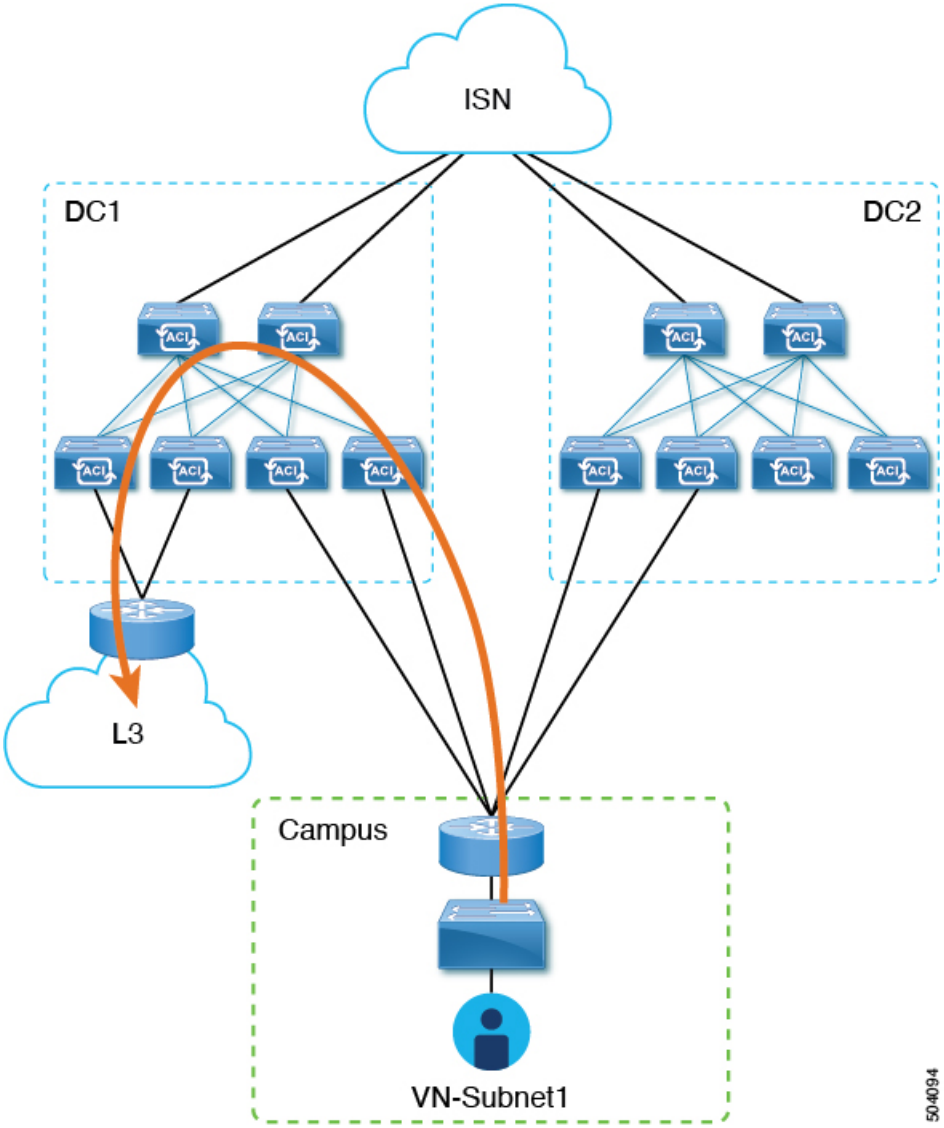
トランジット ルーティングの設定

拡張 SD Access（キャンパス）VN が ACI（データセンター）VRF にマッピングされると、「外部でアドバタイズされる」フラグと「VRF 間で共有される」フラグが構成されている DC VRF の BD サブネットは、「共通」テナント VRF にリークされ、それから SD Access ドメインに向けてアドバタイズされます。これにより、キャンパス ユーザーは DC VRF でプロビジョニングされたアプリケーションにアクセスできるようになります。

（注） SD Access VN が複数の ACI VRF にマッピングされている場合、マッピングされたすべての ACI VRF で重複しないプレフィックスのみを「VRF 間で共有」として構成する必要があります。

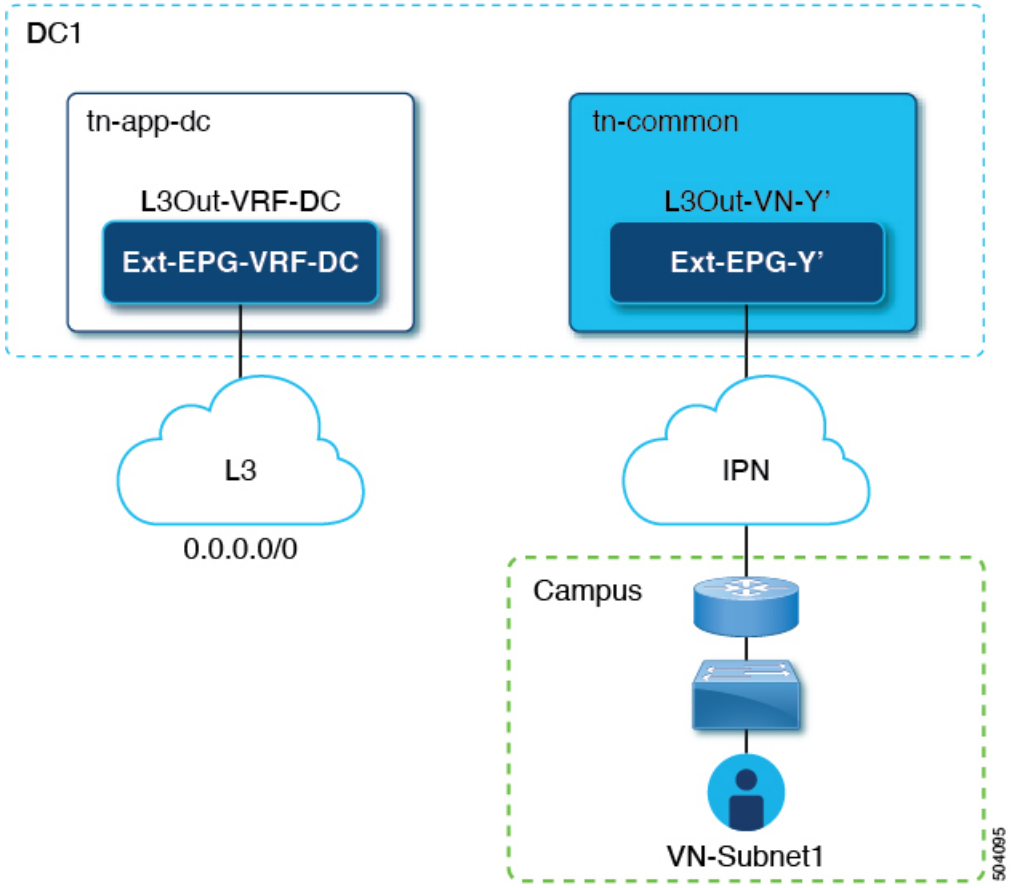
これらの BD サブネットのアドバタイズに加えて、キャンパス ユーザーが ACI ドメインをトランジットとして使用して外部 L3 ネットワーク ドメインにアクセスする必要がある場合があります（図 4 : トランジットとしての ACI ドメイン （18 ページ））。

図 *4*: トランジットとしての *ACI* ドメイン



このシナリオでは、DC VRF（L3Out-DC-VRF）に関連付けられた L3Out 接続は、外部ドメインへの接続を許可するためにプロビジョニングされ、外部ルート（図 5 : L3Out 接続 （19 ページ） の例では単純な 0.0.0.0/0 デフォルト）が DC VRF ルーティング テーブル（tn-app-dc の一部）にインポートされます。

図 *5 : L3Out* 接続



キャンパス ユーザーがデータセンター経由で外部 L3 ドメインに接続できるようにするには、外部ルートを uncommon VRF にリークして、DC へのキャンパス VN 拡張のため自動生成された L3Out 接続（L3Out-VN-Y'）を介してキャンパス ドメインに向けてアドバタイズできるようにする必要があります。

外部ルートのリークを有効にするには、次の手順に従います。

始める前に

拡張キャンパス VN をデータセンター VRF にマッピングし、接続を確立しておく必要があります。

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

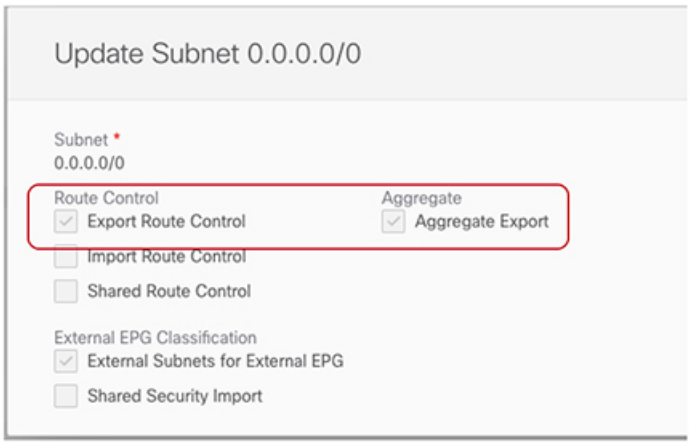
ステップ 2 左のナビゲーション ペインで、**[管理（Admin）] > [統合（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

ステップ 4 正常にマッピングされたキャンパス VN の行で、アクション メニュー（[...]）をクリックし、[トランジット ルートを有効にする（Enable Transit Route）] を選択します。

この構成（図 6 : エクスポート ルート制御 （20 ページ））は、Ext-EPG-Y' の下に 0.0.0.0/0 プレフィックスを作成し、次の「ルート制御」フラグを設定して、tn-app-dc テナントからリークされたすべての外部ルートの IPN へのアドバタイジングを許可します。

図 *6 :* エクスポート ルート制御



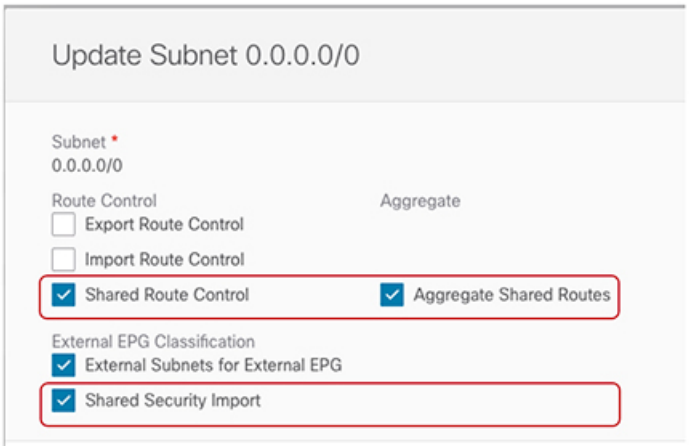
トランジット ルーティングを無効にするには、アクション メニュー（[...]）をクリックし、[トランジット ルートを無効にする（Disable Transit Route）] を選択します。

（注） いずれかの設定（有効または無効）で、キャンパス サイトは ACI VRF 内部の共有 BD サブネットにアクセスできます。

ステップ 5 左のナビゲーション ペインから、**[構成（Configure）」] > [テナント テンプレート（Tenanat Template）] > [アプリケーション（Applications）] > [スキーマ（Schemas）]** を選択し、データセンター テナント アプリケーションを構成するためのテンプレートに移動します。

ステップ 6 データセンター テナント アプリケーション テンプレートで、DC VRF の Ext-EPG-VRF-DC に関連付けられた 0.0.0.0/0 プレフィックスの下にフラグを設定して、インターネットから学習した外部ルートを uncommon にリークできるようにします（図 7 : 共有ルート コントロール （20 ページ））。

図 *7 :* 共有ルート コントロール

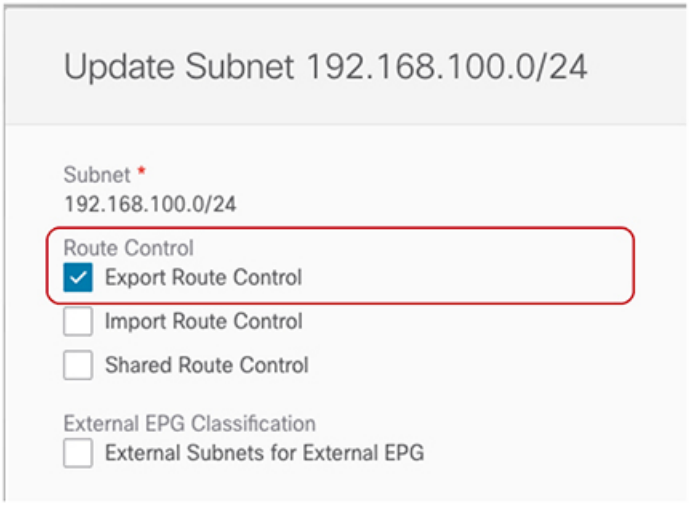


（注） 示されている設定により、L3Out-VRF-DC で受信されたすべての外部プレフィックスが tm-common にリークされるため、キャンパス ドメインに向けてアドバタイズされます。この設定により、L3 ドメインから受信した場合、0.0.0.0/0 デフォルト ルートのリークも許可されます。必要に応じて、外部プレフィックスのサブセットのみを uncommon にリークできる、より詳細な構成を適用できます。これは、プレフィックスのこれらのサブセットに一致する特定のエントリを作成し、それらのエントリに「ここに」示されているのと同じフラグ構成を適用することによって実現されます。

ステップ 7 データセンター テナント アプリケーション テンプレートで、外部 L3 ドメインに向けてアドバタイズされるキャンパス VN サブネット（またはサブネットのセット）に一致する Ext-EPG-VRF-DC の下に特定のプレフィックスを定義します。

図 8 : サブネットの更新 （21 ページ） に示す例では、この設定は特定の 192.168.100.0/24 プレフィックスに適用されます。

図 *8* : サブネットの更新



（注） VN サブネットに個別のプレフィックスを作成すると、外部 L3 ドメインへのキャンパス VN サブネットのアドバタイズを最も詳細なレベルで制御できます。このような細かい制御が必要ない場合は、代わりに 0.0.0.0/0 プレフィックスに関連付けられた「ルート制御のエクスポート」フラグを設定できます。これにより、uncommon から tn-app-dc に漏えいしたすべてのキャンパス VN サブネットを外部ドメインに送信できます。

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。