VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

- VXLAN BGP EVPN ファブリックのマルチサイト ドメイン , on page 1
- MSD およびメンバー ファブリックのプロセス フロー （3 ページ）
- MSD ファブリックの作成とメンバー ファブリックの関連付け （6 ページ）
- MSD ファブリックでのネットワークと VRF の作成と展開 （12 ページ）
- スタンドアロン ファブリック（既存のネットワークと VRF を使用）を MSD ファブリックに移動する , on page 14
- マルチサイト展開での CloudSec のサポート （15 ページ）

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

マルチサイト ドメイン（MSD）は、複数のメンバー ファブリックを管理するために作成されるマルチファブリック コンテナです。MSD は、メンバー ファブリック間で共有されるオーバーレイ ネットワークと VRF を定義するための単一の制御ポイントです。ファブリック（マルチファブリック オーバーレイ ネットワーク ドメインの一部として指定されている）をメンバー ファブリックとして MSD の下に移動すると、メンバー ファブリックは、MSD レベルで作成されたネットワークと VRF を共有します。このようにして、一度にさまざまなファブリックのネットワークと VRF を、一貫した仕方でプロビジョニングできます。複数のファブリック プロビジョニングに関連する時間と複雑さが大幅に削減されます。

サーバー ネットワークと VRF はメンバー ファブリック全体で（1 つの拡張ネットワークとして）共有されるため、新しいネットワークと VRF のプロビジョニング機能は MSD ファブリック レベルで提供されます。新しいネットワークと VRF の作成は、MSD に対してのみ許可されます。すべてのメンバー ファブリックは、MSD 用に作成された新しいネットワークと VRF を継承します。

MSD ファブリックのトポロジ ビューには、すべてのメンバー ファブリックと、それらが互いにどのように接続されているかが、1 つのビューとして表示されます。各メンバー ファブリックの展開画面に個別にアクセスして展開する代わりに、単一のトポロジ展開画面から、メンバー ファブリックにオーバーレイ ネットワーク（および VRF）を展開できます。

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

Note

- Cisco NDFC の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。
- BGW vPC のペアリングを解除した後、メンバー ファブリックで**構成の再計算**と**構成の展開**を実行し、続いて MSD ファブリックの**構成の再計算**と**構成の展開**を実行します。

ファブリック固有の用語：

- **スタンドアロン ファブリック**：MSD の一部ではないファブリックは、MSD の観点からスタンドアロン ファブリックと呼ばれます。MSD の概念が登場する前は、すべてのファブリックはスタンドアロンと見なされていましたが、現在は、2 つ以上のファブリックを相互に接続できます。
- **メンバー ファブリック**：MSD の一部であるファブリックは、メンバー ファブリックまたはメンバーと呼ばれます。最初にスタンドアロン ファブリック（タイプ *Easy_Fabric*）を作成してから、それを MSD 内へ移動してメンバー ファブリックにします。

スタンドアロン ファブリックが MSD に追加されると、次のアクションが実行されます。

- スタンドアロン ファブリックの関連属性とネットワークおよび VRF 定義が、MSD でも同様にチェックされます。競合がある場合、MSD へのスタンドアロン ファブリックの追加は失敗します。競合がない場合、スタンドアロン ファブリックは MSD のメンバー ファブリックになります。競合がある場合、競合の詳細が MSD ファブリックの保留中のエラーログに記録されます。競合を解決してから、スタンドアロン ファブリックを MSD に再度追加してみることができます。
- MSD に存在していなかったスタンドアロン ファブリックからのすべての VRF およびネットワークの定義は、MSD にコピーされ、他の既存の各メンバー ファブリックに継承されます。
- MSD からの VRF とネットワーク（およびその定義、つまりスタンドアロン ファブリックには存在していなかった MSD の VRF、L2 および L3 VNI パラメータなど） は、メンバーになったばかりのスタンドアロン ファブリックに継承されます。

ファブリックとスイッチのインスタンス変数

MSD はネットワークおよび VRF 値のグローバル範囲をプロビジョニングしますが、ファブリック固有のパラメータや、スイッチ固有のパラメータもあります。そのようなパラメータは、ファブリック インスタンス変数およびスイッチ インスタンス変数と呼ばれます。

ファブリック インスタンスの値は、[VRFs and Networks] ウィンドウからのファブリック コンテキストでのみ編集または更新できます。適切なファブリックをダブルクリックして**ファブリックの概要**を表示し、**[ネットワーク（Networks）]**または**[VRF]**タブを選択します。ファブリック インスタンス変数の例には、BGP ASN、ネットワークごとのマルチキャスト グループ

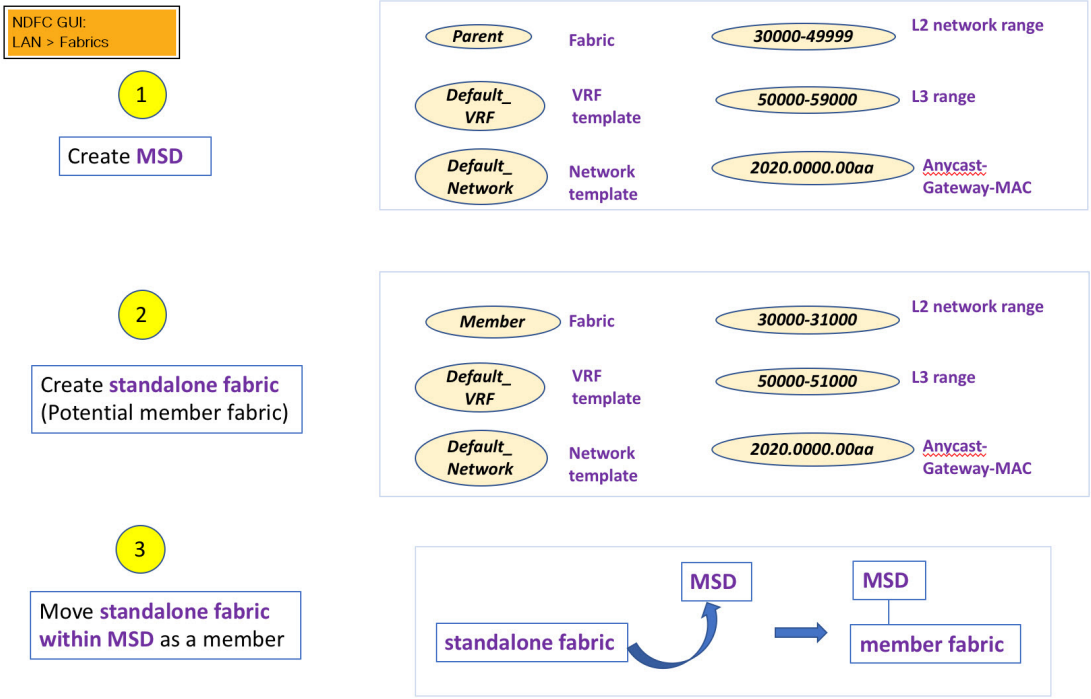
またはVRFなどがあります。マルチキャスト グループ アドレスの編集方法については、MSD ファブリックでのネットワークの作成, on page 13を参照してください。

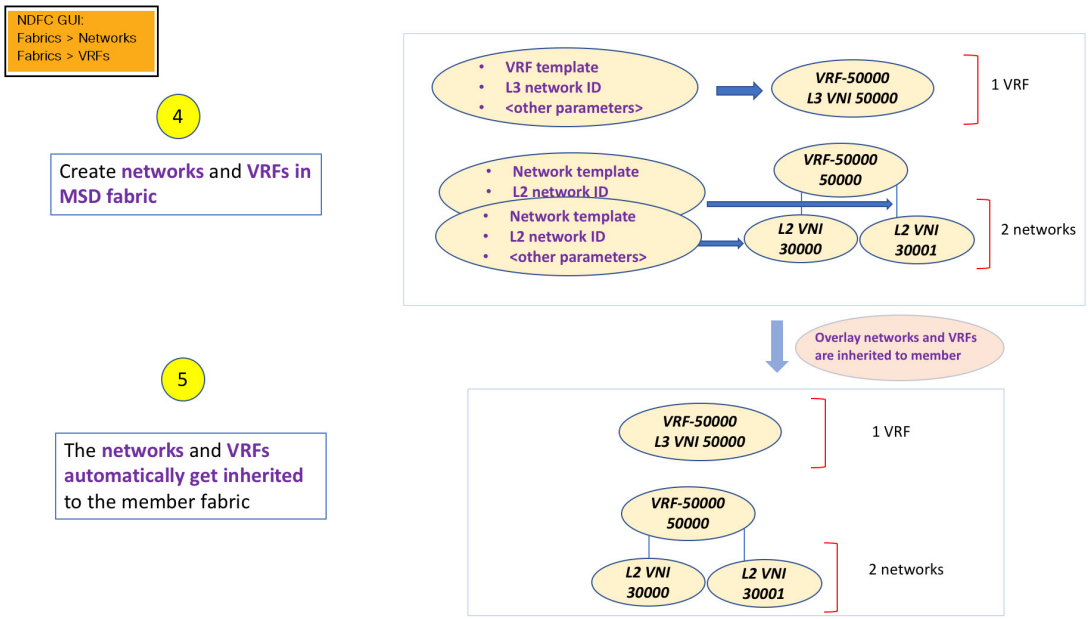
スイッチインスタンスの値は、スイッチにネットワークを展開するときに編集できます。例としては、*VLAN ID* があります。

MSD およびメンバー ファブリックのプロセス フロー

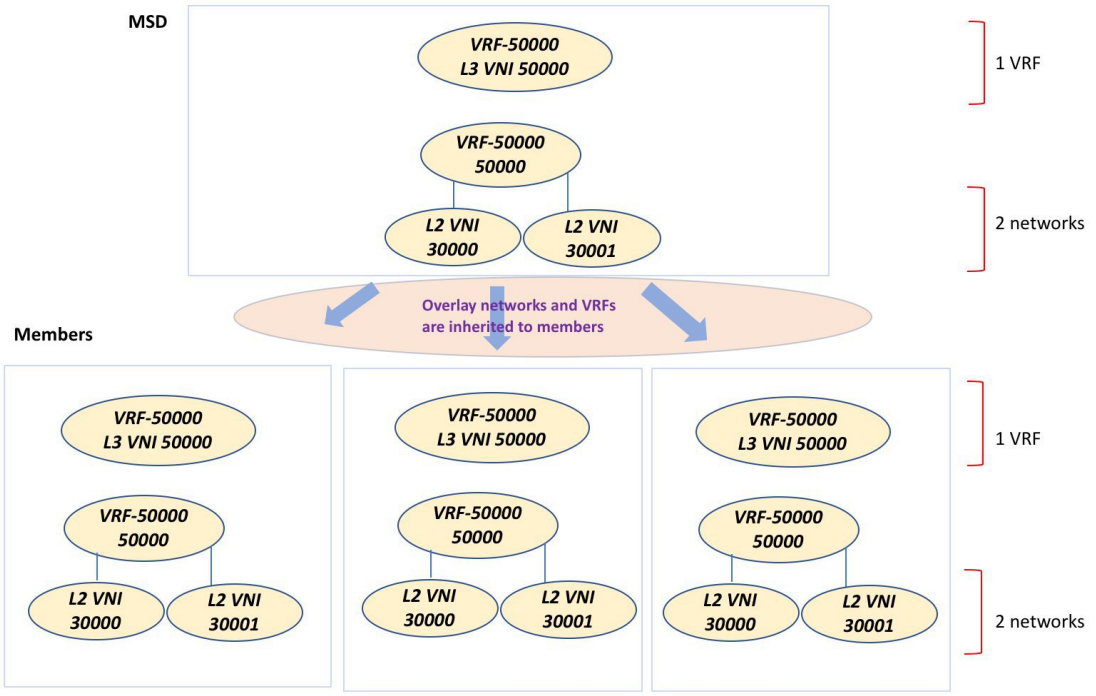
MSDには複数のサイトがあります（したがって、MSDの下に複数のメンバー ファブリックがあります）。MSD用にVRFとネットワークが作成され、メンバー ファブリックに継承されます。たとえば、VRF-50000（およびID 50000のL3ネットワーク）と、ID 30000および30001のL2ネットワークが、MSDに対して一度に作成されます。

MSD とメンバー ファブリックの作成、およびMSDからメンバー ファブリックへの継承プロセスの概要フロー チャート：

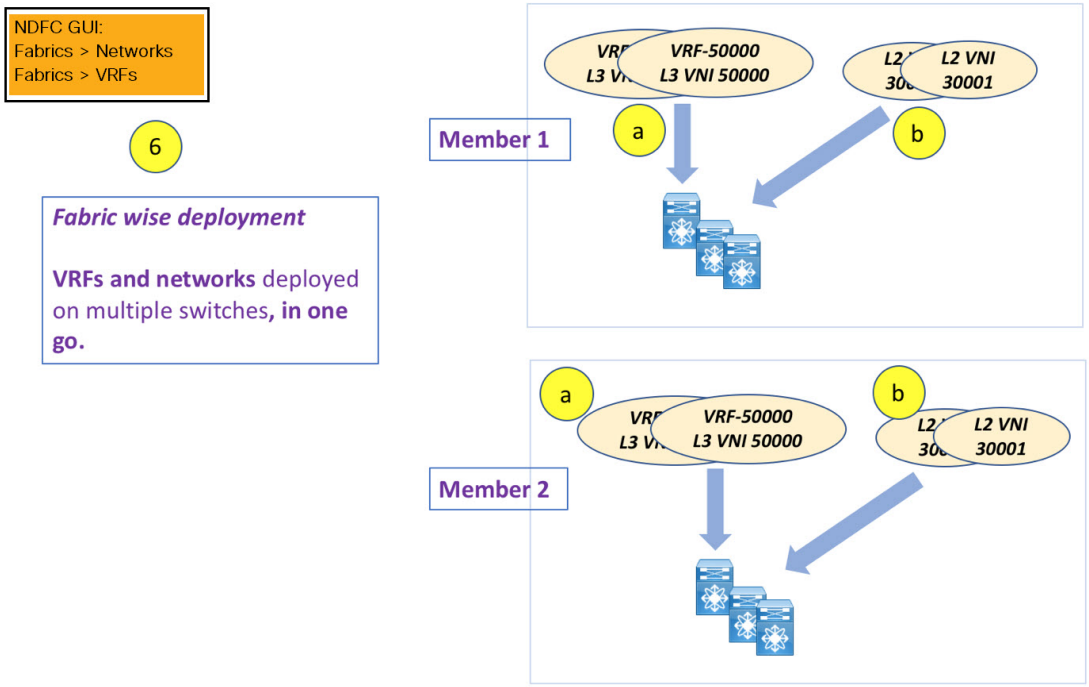




サンプル フローでは、MSD から 1 つのメンバーへの継承について説明しました。MSD には複数のサイトがあります（したがって、MSD の下に複数のメンバー ファブリックがあります）。MSD から複数のメンバーへのサンプル フロー：



この例では、VRF-50000（および ID 50000 の L3 ネットワーク）と、ID 30000 および 30001 の L2 ネットワークが、一度に作成されます。図に示すように、ネットワークと VRF はメンバー ファブリック スイッチに順次展開されます。



単一の MSD 展開画面からオーバーレイ ネットワークをプロビジョニングできます。

（注） 既存のネットワークと VRF を持つスタンドアロン ファブリックを MSD に移行すると、NDFC は適切な検証を行います。これについては、次のセクションで詳しく説明します。

ドキュメントの今後のセクションでは、以下について説明します。

- MSD ファブリックの作成。
- （潜在的なメンバーとしての）スタンドアロンファブリックの作成と、メンバーとしての MSD の下でのその移行。
- MSD でのネットワークと VRF の作成、およびメンバー ファブリックへの継承。
- MSD およびメンバー ファブリック トポロジ ビューからのネットワークと VRF の展開。
- ファブリック移行のその他のシナリオ：
  - 既存のネットワークおよび VRF を持つスタンドアロン ファブリックの MSD ファブリックへの移行。
  - ある MSD のメンバー ファブリックの、別の MSD への移行。

MSDファブリックの作成とメンバーファブリックの関連付け

このプロセスは、次の 2 つのステップで説明されます。

1. MSD ファブリックを作成します。
2. 新しいスタンドアロン ファブリックを作成し、メンバー ファブリックとして MSD ファブリックの下に移動します。

MSD ファブリックの作成

1. **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

2. ファブリックの一意の名前を入力します。

   [テンプレートを選択（Choose Template）] をクリックして、ファブリックのテンプレートを選択します。

   使用可能なすべてのファブリック テンプレートのリストが表示されます。

3. ファブリック テンプレートの使用可能なリストから、**MSD_Fabric** テンプレートを選択します。

   [選択（Select）] をクリックします。

   ファブリックを作成するために必要なフィールド値を入力します。

   画面のタブとそのフィールドについては、以降のポイントで説明します。オーバーレイおよびアンダーレイ ネットワーク パラメータは、これらのタブに含まれています。

4. **[一般パラメータ（General Parameters）]** タブでは、すべてのフィールドにデータが自動入力されます。フィールドは、レイヤ2およびレイヤ3 VXLANセグメント識別子の範囲、デフォルトのネットワークおよび VRF テンプレート、およびエニーキャスト ゲートウェイの MAC アドレスで構成されます。必要に応じて、以下のフィールドを更新します。

   [レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）]：レイヤ 2 VXLAN セグメントの ID の範囲。

   [レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：レイヤ 3 VXLAN セグメントの ID の範囲。

   [VRF テンプレート（VRF Template）]：デフォルトの VRF テンプレート。

   [ネットワーク テンプレート（Network Template）]：デフォルトのネットワーク テンプレート。

[VRF 拡張テンプレート（VRF Extension Template）]：デフォルトの VRF 拡張テンプレート。

[ネットワーク拡張テンプレート（Network Extension Template）]：デフォルトのネットワーク拡張テンプレート。

[Anycast-Gateway-MAC]：エニーキャスト ゲートウェイ MAC アドレス。

[マルチサイト ルーティング ループバック ID（Multisite Routing Loopback Id）]：マルチサイト ルーティング ループバック ID は、このフィールドに入力されます。

[Tor 自動展開フラグ（ToR Auto-deploy Flag）]：このチェックボックスをオンにする音、MSD ファブリックで **[再計算と展開（Recalculate and Deploy）]** をクリックしたときに、Easy ファブリックのネットワークと VRF を外部ファブリックの ToR スイッチに自動展開できます。

5. [**DCI**] タブをクリックします。

   該当するフィールドは次のとおりです。

   [Multi-Site Overlay IFC Deploy Method（マルチサイト オーバーレイ IFC 展開方法）]：データ センターを BGW 経由、手動、バックツーバック、またはルート サーバー経由で接続する方法を選択します。

   [マルチサイト ルート サーバー リスト（Multi-Site Route Server List）]：ルート サーバーの IP アドレスを指定します。複数を指定する場合は、IP アドレスをコンマで区切ります。

   [マルチサイト ルート サーバー BGP ASN リスト（Multi-Site Route Server BGP ASN List）]：ルート サーバーの BGP AS 番号を指定します。複数のルート サーバーを指定する場合は、AS 番号をコンマで区切ります。

   [マルチサイト アンダーレイ IFC 自動展開フラグ（Multi-Site Underlay IFC Auto Deployment Flag）]：チェック ボックスをオンにして、自動構成を有効にします。手動構成の場合、チェックボックスをオフにします。

   [復元時間の遅延（Delay Restore Time）]：マルチサイト アンダーレイおよびオーバーレイ コントロール プレーンのコンバージェンス時間を指定します。最小値は 30 秒で、最大値は 1000 秒です。

   [マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。詳細については、マルチサイト展開での CloudSec のサポート （15 ページ）を参照してください。

   [マルチサイト eBGP パスワードを有効にする（Enable Multi-Site eBGP Password）]：マルチサイト アンダーレイ/オーバーレイ IFC の eBGP パスワードを有効にします。

   [eBGP パスワード（eBGP Password）]：暗号化された eBGP パスワードの 16 進文字列を指定します。

   [eBGP 認証キー暗号化タイプ （eBGP Authentication Key Encryption Type）]：BGP キー暗号化タイプを指定します。3DES の場合は **3**、Cisco の場合は **7** です。

6. [リソース（Resources）] タブをクリックします。

[マルチサイト ルーティング ループバック IP 範囲（MultiSite Routing Loopback IP Range）]：EVPN マルチサイト機能に使用されるマルチサイト ループバック IP アドレス範囲を指定します。

各メンバー サイトには、オーバーレイ ネットワークの到達可能性のためにマルチサイト ルーティング ループバック IP アドレスが割り当てられている必要があるため、この範囲から各メンバー ファブリックに一意のループバック IP アドレスが割り当てられます。ファブリックごとのループバック IP アドレスは、特定のメンバー ファブリック内のすべての BGW に割り当てられます。

[DCI サブネット IP 範囲（DCI Subnet IP Range）] および **[サブネット ターゲット マスク（Subnet Target Mask）]**：データ センター インターコネクト（DCI）サブネットの IP アドレスとマスクを指定します。

7. [構成のバックアップ（Configuration Backup）] タブをクリックします。

   [スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

   [スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）] チェックボックスをオンにすると、このフィールドが有効になります。

   両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

   [保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

8. [保存（Save）] をクリックします。

   画面の右下に、新しい MSD ファブリックが作成されたことを示すメッセージが短時間表示されます。ファブリック作成後、ファブリックのページが表示されます。テーブルには、ファブリック名として *[MSD-Fabric]* が表示されます。

   新しい MSD が作成されると、新しく作成された MSD ファブリック インスタンスが [ファブリック（Fabrics）] テーブルに表示されます。

   MSD ファブリックは、*[Multi-Fabric Domain]* として **[ファブリック タイプ（Fabric Type）]** フィールドに表示されます。メンバー ファブリック名がブランチとして含まれています。メンバー ファブリックが作成されていない場合は、スタンドアロン ファブリックとして表示されます。

MSD ファブリックを作成し、メンバー ファブリックをその下に移動する手順は次のとおりです。

1. MSD ファブリックを作成します。
2. **新しいスタンドアロン ファブリックを作成し、メンバー ファブリックとして MSD ファブリックの下に移動します。**

ステップ 1 が完了しました。ステップ 2 については、次のセクションで説明します。

新しいファブリックを作成し、メンバーとして MSD ファブリックの下に移動する

新しいファブリックは、スタンドアロン ファブリックとして作成されます。新しいファブリックを作成したら、メンバーとして MSD の下に移動できます。ベスト プラクティスとして、（MSD の）メンバー ファブリックにする予定の新しいファブリックを作成するときは、ネットワークと VRF をファブリックに追加しないでください。ファブリックを MSD の下に移動してから、MSD のネットワークと VRF を追加します。そうすれば、メンバーと MSD ファブリック ネットワークおよび VRF パラメータ間の検証（または競合解決）の必要がなくなります。

新しいファブリックの作成については、Easy ファブリックの作成プロセスで説明されています。MSD ドキュメントでは、ファブリックの移動について説明されています。ただし、スタンドアロン（メンバーとなる可能性のある）ファブリックについては、いくつかの指針があります。

[リソース（Resource）] タブの値は自動的に生成されます。新しいネットワークおよび VRF の作成に割り当てられる VXLAN VNI ID 範囲（L2 セグメント ID 範囲および L3 パーティション ID 範囲フィールド内）は、MSD ファブリック セグメント ID 範囲からの値です。VXLAN VNI 範囲、または VRF およびネットワーク VLAN 範囲を更新する場合は、次のことを確認します。

- 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。
- 一度に更新できる値の範囲は 1 つだけです。複数の値の範囲を更新する場合は、別のインスタンスで実行します。たとえば、L2 と L3 の範囲を更新する場合は、次の手順を実行する必要があります。
  1. L2 範囲を更新し、[保存（Save）] をクリックします。
  2. [ファブリックの編集（Edit Fabric）] オプションをもう一度クリックし、L3 範囲を更新して [保存（Save）] をクリックします。

[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]、**[ネットワーク テンプレート（Network Template）]**、および**[VRF テンプレート（VRF Template）]** フィールドの値が MSD ファブリックと同じであることを確認します。それ以外の場合、MSD へのメンバー ファブリックの移動は失敗します。

その他の指針：

- メンバー ファブリックにはサイト ID が設定されている必要があり、サイト ID はメンバー間で一意である必要があります。
- BGP AS 番号は、メンバー ファブリックに対して一意である必要があります。
- loopback0 のアンダーレイ サブネット範囲は一意である必要があります。
- loopback1 のアンダーレイ サブネット範囲は一意である必要があります。

[保存（Save）] をクリックすると、ファブリックが作成されたことを示すメモが画面の右下に表示されます。ファブリックが作成されると、ファブリックのページが表示されます。ファブリックのリストにファブリック名が表示されます。

MSD-Parent-Fabric の下での Member1 ファブリックの移動

MSD ファブリックの概要に移動して、その下のメンバー ファブリックを関連付ける必要があります。

1. MSD ファブリック名をダブルクリックして **[ファブリックの概要（Fabric Overview）]** 画面を表示します。
2. **[子ファブリック（Child Fabrics）]** で、**[アクション（Actions）] > [ファブリックを MSD に移動（Move Fabric into MSD）]** をクリックします。

   [ファブリックの概要（Fabric Overview）] > [アクション（Action）] > [子ファブリックの追加（Add Child Fabrics）] をクリックして、メンバー ファブリックを MSD に追加することもできます。

   MSD の一部ではない子ファブリックのリストが表示されます。他の MSD コンテナ ファブリックのメンバー ファブリックは、ここには表示されません。
3. *Member1* ファブリックを MSD ファブリックに関連付けるため、**Member1** ファブリックを選択して **[選択（Select）]** をクリックします。
4. ファブリックを選択し、**[選択（Select）]** をクリックします。

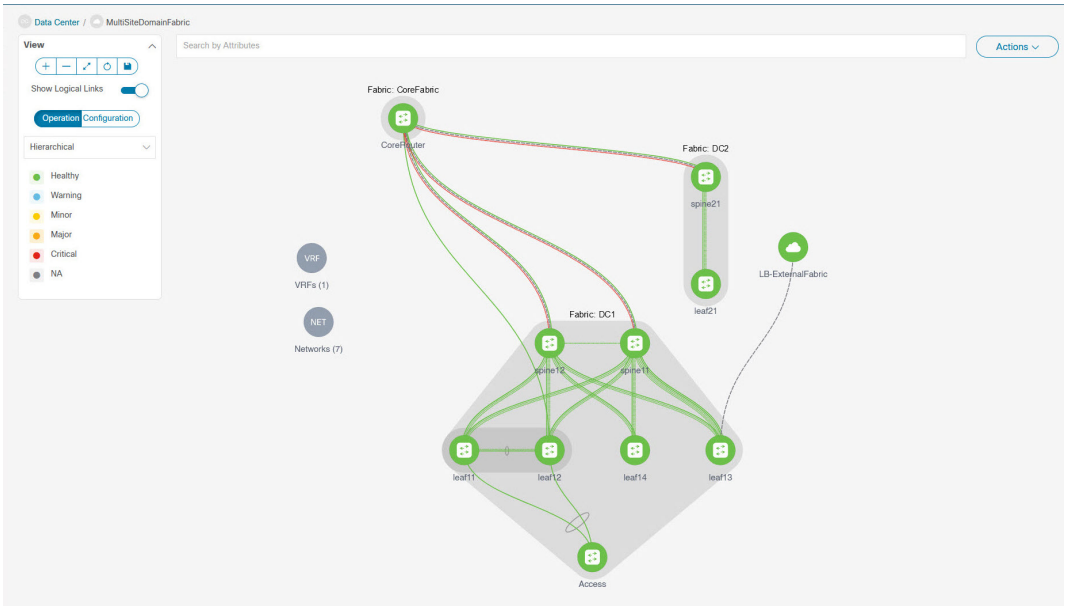
   Member1 が MSD ファブリックに追加され、ファブリック リスト テーブルの **[子ファブリック（Child Fabrics）]** に表示されることがわかります。

MSD ファブリックのトポロジ ビューの指針

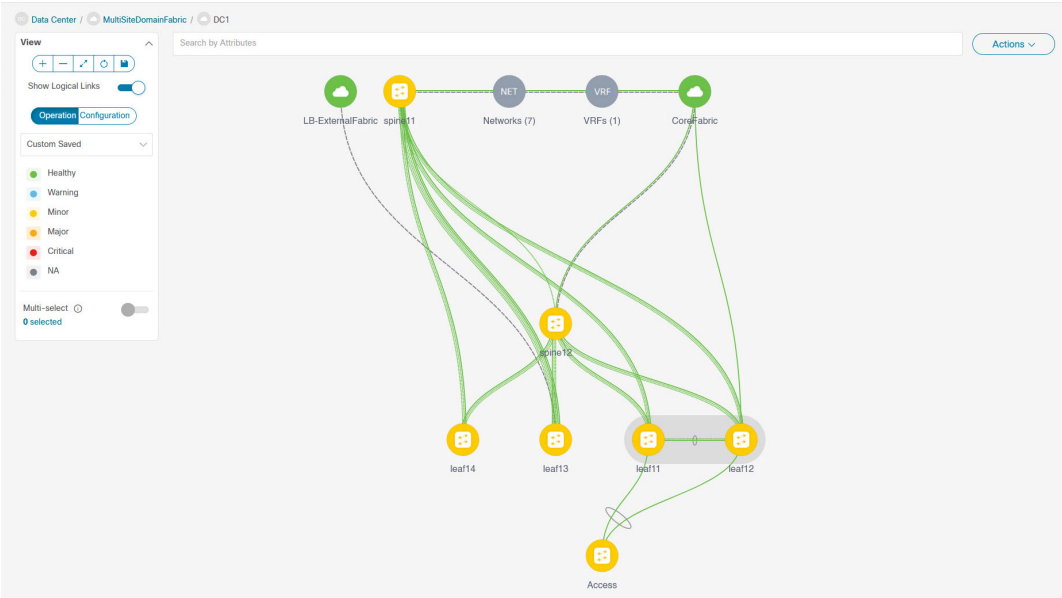
[トポロジ（Topology）] タブには、構成された MSD ファブリックとその子ファブリックが表示されます。

- **[MSD ファブリック トポロジ ビュー（MSD fabric topology view）]**：MSD ファブリックとそのメンバー ファブリックが表示されます。境界は、各メンバー ファブリックを定義します。ファブリックのすべてのファブリック デバイスは、境界に限定されます。

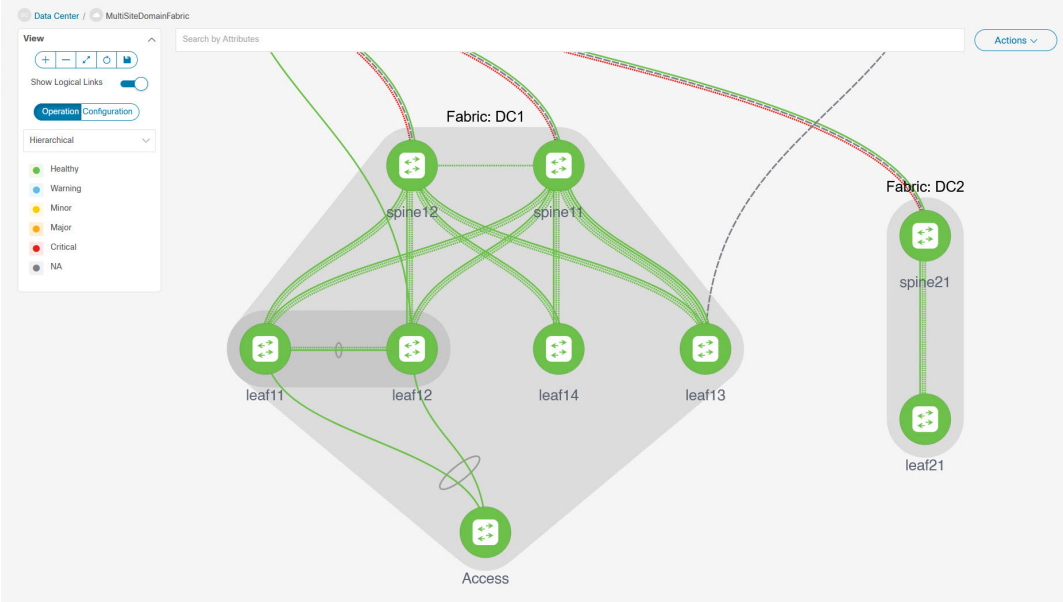
  メンバー ファブリックをダブルクリックして、さらに要素を表示します。



- **[メンバー ファブリック トポロジ ビュー（Member fabric topology view）]**：メンバー ファブリックとそのスイッチが表示されます。また、接続されている外部ファブリックが表示されます。



- 境界は、スタンドアロンVXLANファブリックと、MSDファブリック内の各メンバーファブリックを定義します。ファブリックのデバイスは、ファブリックの境界に限定されます。スイッチのアイコンはドラッグして移動できます。ユーザーエクスペリエンスを向上させるために、NDFCでは、スイッチに加えて、ファブリック全体を移動できます。ファブリックを移動するには、カーソルをファブリック境界内（スイッチ アイコン上ではなく）に置き、目的の方向にドラッグします。



リンクの追加と編集

リンクを追加するには、**[アクション（Actions）] > [その他（More）] > [リンクを追加（Add Link）]**を選択します。リンクを編集するには、**[アクション（Actions）] > [その他（More）] > [リンクを編集（Edit Link）]**を選択します。

異なるファブリックのボーダースイッチ間（ファブリック間）、または同じファブリック内のスイッチ間（ファブリック内）にリンクを追加する方法については、**ファブリックのリンク**のトピックを参照してください。

MSD ファブリックでのネットワークと VRF の作成と展開

スタンドアロンファブリックでは、ファブリックごとにネットワークと VRF が作成されます。MSD ファブリックでは、ネットワークと VRF は MSD ファブリック レベルで作成する必要があります。ネットワークと VRF は、すべてのメンバー ネットワークによって継承されます。メンバー ファブリックのネットワークおよび VRF を作成または削除することはできません。ただし、編集することはできます。

たとえば、2 つのメンバー ファブリックを持つ MSD ファブリックを考えてみます。MSD ファブリックに 3 つのネットワークを作成すると、3 つのネットワークすべてが自動的に両方のメンバー ファブリックで展開できるようになります。

メンバー ファブリックは MSD ファブリックのネットワークと VRF を継承しますが、ファブリックごとにネットワークと VRF を個別に展開する必要があります。

ファブリックごとの展開ビューに加えて、MSD の展開ビューが導入されました。このビューでは、MSD 内のすべてのメンバー ファブリックのオーバーレイ ネットワークを一度に表示

し、プロビジョニングできます。ただし、ファブリックごとにネットワークと VRF の構成を個別に適用して保存する必要があります。

（注） ネットワークと VRF は、サーバー（またはエンド ホスト）がその下でグループ化される共通の識別子（メンバー ファブリック全体で表現される）であり、同じファブリック、それとも異なるファブリックに属しているかにはかかわりなく、ネットワークと VRF ID に基づいてエンド ホスト間でトラフィックを送信できるようにします。メンバー ファブリック全体で共通の表現があるため、ネットワークと VRF を一度にプロビジョニングできます。異なるファブリックのスイッチは物理的にも論理的にも異なるため、ファブリックごとに同じネットワークと VRF を個別に展開する必要があります。

たとえば、2 つのメンバー ファブリックを含む MSD にネットワーク 30000 と 30001 を作成すると、メンバーファブリック用にネットワークが自動的に作成され、展開に使用できるようになります。

30000 および 30001 は、単一の（MSD ファブリック）展開画面を介して、すべてのメンバーファブリックのボーダーデバイスに展開できます。これ以前は、最初のメンバーのファブリック展開画面にアクセスし、ファブリックのボーダー デバイスに 30000 と 300001 を展開してから、2 番目のメンバー ファブリック展開画面にアクセスして、再度展開する必要がありました。

ネットワークと VRF は MSD で作成され、メンバー ファブリックに展開されます。手順は次のとおりです。

1. MSD ファブリックにネットワークと VRF を作成します。
2. メンバー ファブリックのデバイスにネットワークと VRF を展開します。

MSD ファブリックでのネットワークの作成

いくつかのガイドラインと指針：

- MSD ファブリック レベルで **[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** チェックボックスをオンにして、NDFC サービスをアップグレードしようとすると、アップグレード中に MSD ファブリック レベルから自動的に削除されます。
- MSD ファブリック ネットワークでは、**ネットワーク プロファイル**を一部だけ（**[一般（General）]** タブと **[詳細（Advanced）]** タブで）編集することができます。
- MSD には複数のファブリックを含めることができます。これらのファブリックは、マルチキャストまたは入力レプリケーションを介して BUM トラフィックを転送します。すべてのファブリックが BUM トラフィックにマルチキャストを使用する場合でも、これらのファブリック内のマルチキャスト グループは同じである必要はありません。
- MSD でネットワークを作成すると、すべてのメンバー ファブリックに継承されます。ただし、マルチキャスト グループ アドレスは、ファブリック インスタンス ごとの変数です。マルチキャスト グループ アドレスを編集するには、メンバー ファブリックに移動してネットワークを編集する必要があります。**[マルチキャスト グループ アドレス（Multicast**

Group Address）] フィールドの詳細については、スタンドアロン ファブリックのネットワークの作成を参照してください。

- ネットワークを削除できるのは MSD ファブリックからだけであり、メンバー ファブリックからは削除できません。削除する前には、それぞれのファブリック デバイスでネットワークを展開解除する必要があります。
- MSD ファブリックからネットワークを削除すると、そのネットワークはメンバー ファブリックからも自動的に削除されます。

スタンドアロン ファブリックのネットワークの作成を参照してください。

MSD ファブリックでの VRF の作成

メンバーファブリック レベルでVRFを削除することはできません。MSDファブリックでVRFを削除します。削除された VRF は、すべてのメンバー ファブリックから自動的に削除されます。

VRF の作成を参照してください。

MSD およびメンバー ファブリックでのネットワークと VRF の削除

ネットワークを削除できるのは MSD ファブリックからだけであり、メンバー ファブリックからは削除できません。MSD ファブリック内のネットワークおよび対応する VRF を削除するには、次の手順に従います。

1. 削除する前に、それぞれのファブリック デバイスでネットワークを展開解除します。
2. MSD ファブリックからネットワークを削除します。
3. 削除する前に、それぞれのファブリック デバイスで VRF を展開解除します。
4. MSD ファブリックから VRF を削除します。複数の VRF インスタンスを一度に削除することもできます。

（注） MSD ファブリックから VRF を削除すると、メンバー ファブリックからも自動的に削除されます。

スタンドアロン ファブリック（既存のネットワークと VRF を使用）を MSD ファブリックに移動する

既存のネットワークと VRF を持つスタンドアロン ファブリックをメンバーとして MSD ファブリックに移動する場合は、共通のネットワーク（つまり、L2 VNI と L3 VNI 情報）、エニーキャスト ゲートウェイ MAC、VRF とネットワーク テンプレートがファブリックと MSD 全体で同じであることを確認してください。NDFC は、スタンドアロンファブリック（ネットワー

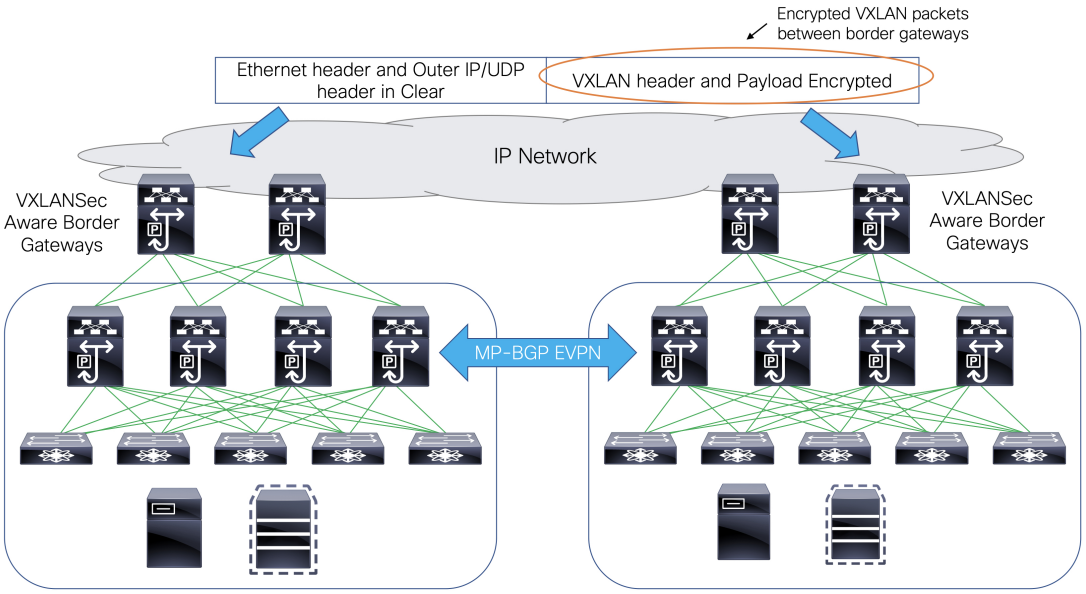
クおよび VRF 情報）を MSD ファブリックの（ネットワークおよび VRF 情報）に対して検証して、エントリの競合を回避します。エントリの競合の例は、2 つの一般的なネットワーク名が異なるネットワーク ID を持っている場合です。検証後、競合がなければ、スタンドアロン ファブリックはメンバー ファブリックとして MSD ファブリックに移動されます。詳細:

- MSD ファブリックは、MSD ファブリックに存在しないスタンドアロン ファブリックのネットワークと VRF を継承します。これらのネットワークと VRF は、メンバー ファブリックによって継承されます。
- 新しく作成されたメンバー ファブリックは、MSD ファブリックのネットワークと VRF（新しく作成されたメンバー ファブリックには存在しないもの）を継承します。
- スタンドアロン ファブリックと MSD ファブリックの間に競合がある場合、検証によって、エラー メッセージが表示されるようにします。更新後、スタンドアロン ファブリックを再度 MSD に移動できます。移動が成功すると、ページの上部に移動が成功したことを示すメッセージが表示されます。

メンバー ファブリックをスタンドアロン ステータスに戻すと、ネットワークと VRF はそのまま残りますが、MSD ファブリックの範囲外で、独立したファブリック内にあるものとして、関連したままになります。

マルチサイト展開での CloudSec のサポート

CloudSec 機能は、異なるファブリック内のボーダー ゲートウェイ デバイス間の送信元から宛先へのパケット暗号化をサポートすることにより、マルチサイト展開で安全なデータセンター相互接続を可能にします。



CloudSec 機能は、Cisco NX-OS リリース 9.3(5) 以降を搭載した Cisco Nexus 9000 シリーズ FX2 プラットフォームでサポートされています。FX2 プラットフォームであり、Cisco NX-OS リ

リース 9.3(5) 以降を実行するボーダー ゲートウェイ、ボーダー ゲートウェイ スパイン、およびボーダー ゲートウェイ スーパースパインは、CloudSec 対応スイッチと呼ばれます。

CloudSec は、MSD ファブリックの作成中に有効にすることができます。

（注） CloudSec セッションは、2 つの異なるサイトのボーダー ゲートウェイ（BGW）間の DCI を介したポイントツーポイントです。サイト間のすべての通信は、VIP の代わりにマルチサイト PIP を使用します。CloudSec を有効にするには、VIP から PIP に切り替える必要があります。これにより、サイト間のデータ フローのトラフィックが中断される可能性があります。したがって、CloudSec の有効または無効の切り替えは、メンテナンス ウィンドウ中に行なうことをお勧めします。

MSD で CloudSec を有効にする

NDFC Web UI で、**[LAN] > [ファブリック（Fabircs）]** を選択します。**[ファブリックの作成（Create Fabric）]** をクリックして新しい MSD ファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックして既存の MSD ファブリックを編集することができます。

[DCI] タブで、CloudSec 構成の詳細を指定できます。

[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。

Cloudsec が MSD レベルで有効になっている場合、NDFC は、すべての Cloudsec 対応ゲートウェイのアップリンクで、**dci-advertise-pip**（**evpn multisite border-gateway**の下） と 、**tunnel-encryption** も有効にします。

[再計算と展開（Recalculate & Deploy）] をクリックすると、ボーダー ゲートウェイ スイッチの **[構成のプレビュー（Preview Config）]** ウィンドウでこれらの構成を確認できます。

（注） ボーダー ゲートウェイに vPC がある場合、または TRM が有効になっている場合、つまり、マルチサイト オーバーレイ IFC で TRM が有効になっている場合、CloudSec はサポートされません。このシナリオで CloudSec が有効になっている場合、適切な警告またはエラー メッセージが生成されます。

[CloudSec キー文字列（CloudSec Key String）]：16 進キー文字列を指定します。**AES_128_CMAC** を選択した場合は 66 文字の 16 進文字列を入力し、**AES_256_CMAC** を選択した場合は 130 文字の 16 進文字列を入力します。

[CloudSec 暗号化アルゴリズム（CloudSec Cryptographic Algorithm）]：**AES_128_CMAC** または **AES_256_CMAC** を選択します。

[CloudSec 強制（CloudSec Enforcement）]：CloudSec を厳密に強制するか、緩和するかを指定します。

[厳密（strict）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合、エラー メッセージが生成され、構成はどのスイッチにもプッシュされません。

[厳密（strict）] が選択されている場合、**tunnel-encryption must-secure** CLI が MSD 内の CloudSec 対応ゲートウェイにプッシュされます。

[緩和（loose）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合は、警告メッセージが生成されます。この場合、CloudSec 構成は、CloudSec をサポートするスイッチにのみ展開されます。**[緩和（loose）]** が選択されていて、**tunnel-encryption must-secure** CLI が存在する場合は削除されます。

（注） CloudSec をサポートするボーダー ゲートウェイを備えた MSD には、少なくとも 2 つのファブリックが必要です。CloudSec 対応デバイスを備えたファブリックが 1 つしかない場合は、次のエラー メッセージが生成されます。

CloudSec には、CloudSec をサポートできるサイトが少なくとも 2 つ必要です（CloudSec needs to have at least 2 sites that can support CloudSec）。

このエラーを解消するには、CloudSec をサポートするか、CloudSec を無効にできるサイトが少なくとも 2 つあるという条件を満たす必要があります。

[CloudSec ステータス レポート タイマー（CloudSec Status Report Timer）]：CloudSec 動作ステータス定期レポート タイマーを分単位で指定します。この値は、NDFC がスイッチから CloudSec ステータス データをポーリングする頻度を指定します。デフォルト値は 5 分で、範囲は 5 ～ 60 分です。

NDFC の CloudSec 機能を使用すると、MSD 内のすべてのゲートウェイが同じキーチェーン（および 1 つのキー文字列のみ）を持ち、ポリシーを持つようにすることができます。NDFC に 1 つのキー チェーン文字列を指定して、キー チェーン ポリシーを形成することができます。NDFC は、すべてのデフォルト値を使用して encryption-policy を形成します。NDFC は、同じキー チェーン ポリシー、同じ暗号化ポリシー、および暗号化ピア ポリシーを各 CloudSec 対応ゲートウェイにプッシュします。各ゲートウェイには、CloudSec 対応で、同じキーチェーンと同じキー ポリシーを使用する encryption-peer ポリシーが、リモート ゲートウェイごとに 1 つあります。

MSD ファブリック全体に同じキーを使用したくない場合、またはすべてのサイトのサブセットでのみ CloudSec を有効にしたい場合は、**switch_freeform** を使用して、CloudSec 構成をスイッチに手動でプッシュできます。

switch_freeform のすべての CloudSec 構成をキャプチャします。

たとえば、次の設定は **switch_freeform** ポリシーに含まれています。

```
feature tunnel-encryption
evpn multisite border-gateway 600
  dci-advertise-pip
tunnel-encryption must-secure-policy
tunnel-encryption policy CloudSec_Policy1
```

```
tunnel-encryption source-interface loopback20
key chain CloudSec_Key_Chain1 tunnel-encryption
  key 1000
   key-octet-string 7 075e731f1a5c4f524f43595f507f7d737062677147524054590 70b0b0701585440

    cryptographic-algorithm AES_128_CMA
tunnel-encryption peer-ip 192.168.0.6
  keychain CloudSec_Key_Chain1 policy CloudSec_Policy1
```

次のような構成を生成するアップリンク インターフェイス ポリシーのフリーフォーム構成に **tunnel-encryption** を追加します。

```
interface ethernet1/13
  no switchport
  ip address 192.168.1.14/24 tag 54321
  evpn multisite dci-tracking
  tunnel-encryption
  mtu 9216
  no shutdown
```

詳細については、ファブリック スイッチでのフリーフォーム設定の有効化を参照してください。

CloudSec 設定がスイッチに追加または削除されると、DCI アップリンクがフラップし、マルチサイト BGP セッション フラッピングがトリガーされます。既存のクロス サイト トラフィックがあるマルチサイトの場合、この移行中にトラフィックの中断が発生します。したがって、メンテナンス期間中に移行を行うことをお勧めします。

CloudSec 構成の MSD ファブリックを NDFC に移行する場合、Cloudsec 関連の構成は、**switch_freeform** および interface freeform 構成でキャプチャされます。MSD ファブリック設定で Multi-Site Cloudsec をオンにする必要はありません。さらにファブリックを追加し、既存のものとキーを含む同じ CloudSec ポリシーを共有する CloudSec トンネルを確立する場合は、MSD ファブリック設定で CloudSec 構成を有効にすることができます。MSD ファブリック設定の CloudSec パラメータは、スイッチの既存の CloudSec 設定と一致する必要があります。CloudSec 構成は既にフリーフォーム構成に取り込まれており、MSD で CloudSec を有効にすると構成インテントも生成されます。したがって、二重のインテントが生じます。たとえば、MSD 設定で CloudSec キーを変更する場合、NDFC は **switch_freeform** の構成を変更しないため、CloudSec フリーフォーム構成を削除する必要があります。そうしないと、MSD ファブリック設定のキーがフリーフォーム構成のキーと競合します。

CloudSec の動作状態の表示

MSD ファブリックで CloudSec が有効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** を使用して CloudSec セッションの操作ステータスを確認できます。

手順

ステップ 1 MSD ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** > **[詳細ビュー（Detailed View）]**を選択します。

ステップ 3 **[リンク（Link）]** タブをクリックし、左側の **[CloudSec 操作ビュー（CloudSec Operational View）]** タブを選択します。

ステップ 4 CloudSec が無効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** は表示されません。

[操作ビュー（Operational View）] には、次のフィールドと説明があります。

フィールド	説明
Fabric Name（ファブリック名）	CloudSec セッションを持つファブリックを指定します。
セッション	CloudSecセッションに関係するファブリックとボーダー ゲートウェイ スイッチを指定します。
リンクステータス	CloudSec セッションのステータスを指定します。この状態は次のいずれかになります。 • Up：スイッチ間で CloudSec セッションが正常に確立されています。 • Down：CloudSec セッションは動作していません。
稼働時間	CloudSec セッションの稼働時間を指定します。具体的には、最後の Rx および Tx セッションがフラップしてからの稼働時間であり、2 つのセッションのうち小さい方の値が表示されます。
動作理由	CloudSec セッション状態のダウン理由を指定します。

（注） ファブリックで CloudSec が有効になった後、セッションが作成され、次のステータス ポーリングが発生するまでは、動作ステータスを使用できない場合があります。

CloudSec セッションのトラブルシューティング

CloudSec セッションが停止している場合は、プログラマブル レポートを使用してその詳細を確認できます。

手順

ステップ 1 NDFC Web UI で、**[操作（Operations）] [プログラマブル レポート（Programmable Reports）]** を選択します。

ステップ 2 [Create Report] をクリックします。

ステップ 3 **[レポート名（Report Name）]** フィールドにレポート ジョブの一意な名前を入力します。

ステップ 4 **[テンプレートの選択（Select Template）]** ドロップダウン リストから、**fabric_cloudsec_oper_status** を選択します。

ステップ 5 **[次へ（Next）]** をクリックして、**[ソースと繰り返し（Source & Recurrence）]** タブを表示します。

ステップ 6 **[繰り返し（Recurrence）]** フィールドで、レポート ジョブを実行する頻度を選択します。

ステップ 7 レポートを電子メールで送信する場合は、**[電子メールレポート先（Email Report To）]** フィールドに電子メールの ID またはメーラーの ID を入力します。

[設定（Settings）] [サーバ設定（Server Settings）] [SMTP] タブで SMTP を設定する必要があります。データ サービスの IP アドレスがプライベート サブネットにある場合は、SMTP サーバーのスタティック管理ルートを Cisco Nexus Dashboard クラスタ設定に追加する必要があります。

ステップ 8 **[ファブリックの選択（Select fabric(s)）]** テーブルで、レポート ジョブを実行する MSD ファブリックを選択します。

ステップ 9 [保存（Save）] をクリックします。

レポート ジョブは、構成された間隔で実行されます。

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。