拡張クラシック LAN、リリース 12.2.2

目次

新規情報および変更情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.2.2	QKD を使用した MACsec でのファブリック間リンクを使用したファブリック接続のサポート サーバまたは事前共有キー	この機能を使用すると、量子キー流通（QKD）サーバを使用して Media Access Control Security （MACsec ）とファブリック間リンクを使用して 2 つのファブリックを接続し、暗号化キーを安全に交換できます。NDFC 12.2.2 以降、NDFC は、次のファブリックタイプのファブリック間リンクの QKD を使用した MACsec のサポートを追加しました。 ・データ センター VXLAN EVPN ・拡張クラシック LAN ・外部接続ネットワーク NDFC 12.2.2 より前のバージョンでは、NDFC は Data CenterVXLAN EVPN ファブリックおよび BGP ファブリックのファブリック内リンクの MACsec をサポートしていました。 この機能により、NDFC は **[セキュリティ（Security）]** タブを追加しました。詳細については、「セキュリティ」を参照してください。QKD の有無にかかわらず MACsec の構成の詳細については、「 QKD を使用して、2 つのファブリックを MACsec と接続する （ Connecting Two Fabrics with MACsec Using QKD）」を参照してください。
NDFC リリース 12.2.2	vPC/ポートチャネル識別子範囲の割り当て とカスタム vPC/PO 識別子 の指定 のサポート	この機能を使用すると、集約アクセスペアリングに 1 つのリモート対応ポートチャネル（vPC）/ポート チャネル ID 範囲を割り当てることができ、拡張クラシック LAN ファブリックでカスタム vPC/PO ID を指定できます。 NDFC 12.2.2 以降、NDFC は、アクセスおよび集約 vPC/ポート チャネル ID を編集するための **[アクセスペアリング（Access Pairing）]** ページに **[アクション（Action）] > [ペアリングの編集（Edit Pairing）]** オプションを追加しました。 詳細については、「集約アクセス ペアリング用の特定の vPC/ポート 」を参照してください。

拡張クラシック LAN ファブリックの作成

このドキュメントでは、拡張クラシック **LAN** ファブリック テンプレートを使用して新しい拡張クラシック LAN ファブリックを作成する方法について説明します。

このドキュメントでは、拡張クラシック **LAN** ファブリックテンプレートに表示されるフィールドに特化した情報を提供することに注意してください。拡張クラシック **LAN** ファブリック テンプレートを使用した NDFC でのレガシー/クラシック ネットワークの管理に関する詳細な手順については、「Managing Legacy/Classic Networks in Cisco Nexus Dashboard Controller」ドキュメントを参照してください。

1. **[LAN** ファブリック（**LAN Fabrics)]** ページ に移動します：

   [管理（**Manage**）**] > [**ファブリック（**Fabrics**）**]**

2. **[**アクション（**Action**）**] > [**ファブリックを作成（ **Create Fabric**）**]**をクリックします。

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

3. **[**ファブリック名（**Fabric Name**）**]** フィールドにファブリックの一意の名前を入力し、

   [ファブリックの選択（**Choose Fabric**）**]** をクリックします。 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。

4. ファブリック テンプレートの使用可能なリストから、拡張クラシック **LAN** テンプレートを選択し、**[**選択（**Select**）**]** をクリックします。
5. 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、次のセクションで説明されています。ファブリック レベルのパラメータは、これらのタブに含まれています。

   - 一般的なパラメータ
   - スパニングツリー
   - vPC
   - Protocols
   - セキュリティ
   - 詳細設定
   - 関連資料
   - 管理性（Manageability）
   - ブートストラップ
   - コンフィギュレーションのバックアップ
   - Flow Monitor
6. 必要な構成が完了したら **[**保存（**Save**）**]** をクリックします。
   - [ファブリック（Fabric）] をクリックして、スライドイン ペインに概要を表示します。
   - **[**起動（**Launch**）**]** アイコンをクリックして、**[**ファブリックの概要（**Fabric Overview**）**]** を表示します。

一般的なパラメータ

デフォルトでは、[全般パラメータ（**General Parameters**）] タブが表示されます。次のテーブルにこのタブのフィールドが説明されています。

フィールド	説明
First Hop Redundancy Protocol（FHRP）	FHRP プロトコルを指定します。オプションは、次のとおりです。 ・なし（**none**）レイヤ 2 のみが必要な場合は、このオプションを選択します。 ・**hsrp** ・**vrrp** ・**vrrpv3**
ルーティング プロトコル	VRF-Lite Agg-Core/Edge または Collapsed Core：WAN ピアリング プロトコル オプションを指定します。オプションは、次のとおりです。 ・**ebgp** ・**ospf** ・**none**：**none** オプションが選択されている場合、NDFC はピアリングプロトコルを設定しません。必要に応じて、このオプションを使用してピアリング プロトコルを手動で設定する必要があります。
BGP ASN	このフィールドは、*ルーティングプロトコル*で **ebgp** を選択した場合に編集可能になります。 field. ファブリックが関連付けられている BGP AS 番号を入力します。これは、既存のファブリックと同じである必要があります。
パフォーマンス モニタリングを有効化（**EnablePerformance Monitoring**）	オンにすると、パフォーマンス モニタリングが有効になります。 スイッチのコマンド ライン インターフェイスからインターフェイス カウンタをクリアしないでください。インターフェイス カウンタをクリアすると、パフォーマンス モニターにトラフィック使用率に関する誤ったデータが表示される可能性があります。カウンタをクリアする必要があり、スイッチに clear counters コマンドと clear counters snmp コマンドの両方がある場合（すべてのスイッチに clear counters snmp コマンドがあるわけではない）、main コマンドと SNMP コマンドの両方を同時に実行してください。たとえば、clear counters interface ethernet slot/port コマンドを実行し、clear counters interface ethernet slot/port snmp コマンドを実行する必要があります。これにより、1 回限りのスパイクが発生する可能性があります。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら [保存（**Save**）] をクリックします。

スパニングツリー

次の表では、[スパニング ツリー（**Spanning Tree** ）] タブのフィールドについて説明します。すべてのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
スパニング ツリー ルート ブリッジ プロトコル（**Spanning Tree Root Bridge Protocol**）	ルート ブリッジの設定に使用するプロトコルを指定します。オプションは次のとおりです。 ・**rpvst+**：VLAN ごとの高速スパニング ツリー（RPVST） ・**mst**：多重スパニング ツリー ・**unmanaged**（デフォルト）：NDFC によって管理されない STP ルート スパニングツリー設定とブリッジ構成は、集約レイヤのみで適用できます。
スパニングツリー **VLAN** 範囲（**Spanning Tree VLAN Range**）	VLAN 範囲を指定します。例： 1, 3-5, 7, 9-11 デフォルト値は 1 ~ 3967 です。集約デバイスにのみ適用されます。
MST インスタンス範囲（**MST Instance Range**）	MST インスタンス範囲を指定します。例：0- 3,5,7-9 デフォルト値は 0 です。集約デバイスにのみ適用されます。
スパニング ツリー ブリッジ優先度（**Spanning Tree Bridge Priority**）	スパニング ツリーのブリッジ優先度を 4096 の倍数で指定します。集約デバイスにのみ適用されます。
スパニング ツリー **Hello** 間隔（**Spanning Tree Hello Interval**）	構成スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）の生成間隔を秒数で設定します。 デフォルト値は 2 です。集約デバイスにのみ適用されます。
スパニング ツリー転送遅延（**Delay SpanningTree Forward Delay**）	転送遅延タイマーを秒数で設定します。 デフォルト値は 15 です。集約デバイスにのみ適用されます。
スパニング ツリー 最大エージング間隔（**Spanning Tree Max Age Interval**）	スパニングツリーのブリッジ プロトコル データ ユニット（BPDU）で情報が有効である最大期間を秒数で設定します。 デフォルト値は 20 です。集約デバイスにのみ適用されます。
スパニング ツリー パスコスト方式（**SpanningTree Pathcost Method**）	オプションは、次のとおりです。 ・短（**short**）：（デフォルト）:デフォルトのポート パス コストに 16 ビット ベースの値を使用します。 ・長（**long**）：デフォルトのポート パス コストに 32 ビット ベースの値を使用します。 集約デバイスにのみ適用されます。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[**保存（**Save**）**]** をクリックします。

vPC

次の表では、**[VPC]** タブのフィールドについて説明します。すべてのフィールドは、シスコが推奨するベ

ストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
vPC 自動 回復時間（vPC Auto Recovery Time）	vPC 自動回復タイムアウト時間を秒単位で指定します。 ・最小値：240 ・最大値：3600
vPC 遅延 復元時間（vPC Delay Restore Time）	vPC 遅延復元期間を秒単位で指定します。 ・最小値：1 ・最大値：3600
vPC ピア リンク ポート チャネル ID（vPC Peer Link Port Channel ID）	vPC ピア リンクのポートチャネル ID を指定します。このフィールドのデフォルト値は 500 です。 ・最小値：1 ・最大値：4096
vPC IPv6 ND 同期	vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。デフォルトでチェックボックスはオンになっています。この機能を無効にするには、チェックボックスをオフにします。
vPC ドメイン ID の範囲（vPC Domain Id Range）	新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。
vPC レイヤ 3 ピア ルータ オプション	両方のピアとのピアリング隣接関係を形成するためレイヤ 3 デバイスを有効にします。 両方のピアでこのコマンドを設定します。ピアの 1 つでのみこのコマンドを構成するか、 1 つの ピアで無効にするとレイヤ 3 peer-router の動作状態は無効になります。動作状態が変化すると 通知を受け取ります。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[保存（Save）]** をクリックします。

プロトコル

[プロトコル（Protocols）] タブのフィールドについては、次の表で説明します。ほとんどのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
OSPF プロセス タグ（OSPF Process Tag）	[一般パラメータ（General Parameters）] タブの **[ルーティング プロトコル（Routing Protocol）]** で **ospf** を選択した場合、 このフィールドは編集可能になります。 OSPF ルーティング プロセス タグ（OSPF Routing Process Tag）。最大サイズは 20 です。

フィールド	説明
OSPF エリア **ID**	このフィールドは、次の条件で編集可能になります。 ・ [一般パラメータ（General タブの [ルーティングプロトコル（**Routing** Protocol）] フィールドで **ospf** を選択した場合。 ・ 上記の **[OSPF** プロセス タグ（**OSPF Process Tag**）] フィールドに値を入力した場合。 IP アドレス フォーマットの **OSPF** エリア **ID**。
OSPFv3 プロセス タグ（**OSPFv3 Process Tag**）	[一般パラメータ（General Parameters）] タブの **[**ルーティング プロトコル（**Routing Protocol**）] で **ospf** を選択した場合、 このフィールドは編集可能になります。 **OSPFv3** ルーティング プロセス タグ（**OSPFv3 Routing Process Tag**）最大サイズは 20 です。
OSPFv3 エリア **ID**（**OSPFv3 Area ID**）	このフィールドは、次の条件で編集可能になります。 ・ [一般パラメータ（General タブの [ルーティングプロトコル（**Routing** Protocol）] フィールドで **ospf** を選択した場合。 ・ 上記の **[OSPFv3** プロセス タグ（**OSPFv3 Process Tag**）] フィールドに値を入力した場合。 **OSPDv3** エリア **ID**（**OSPFv3 Area ID**）は IP アドレス フォーマットです。
BGP の有効化（**Enable BGP**）認証	このフィールドは、**ebgp** を [全般パラメータ（General Parameters）] タブの[ルーティング プロトコル] フィールドで を選択した場合に編集可能になります。 BGP 認証を有効にする場合、このチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、**[BGP** パスワード キー暗号化タイプ（**BGP Password Key Encryption Type**）] および **[BGP** ネイバー パスワード（**BGP Neighbor Password**）] フィールドが有効になります。
BGP パスワード キー暗号化タイプ（**BGP Password Key Encryption Type**）	このフィールドは、次の条件で編集可能になります。 ・ [一般 パラメータ（General Parameters）] タブの **[**ルーティング プロトコル（**Routing Protocol**）] フィールドで **ebgp** を選択した場合。 ・ 上記の **[BGP** 認証の有効化（**Enable BGP Authentication**）] フィールドを有効にした場合。 3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

BGP ネイバー パスワード（BGP Neighbor Password）	このフィールドは、次の条件で編集可能になります。 ・[一般 パラメータ（General Parameters）] タブの **[ルーティング プロトコル（Routing Protocol）]** フィールドで **ebgp** を選択した場合。 ・上記の **[BGP 認証の有効化（Enable BGP Authentication）]** フィールドを有効にした場合。 VRF Lite BGP ネイバー パスワードを 16 進数文字列として入力します。
OSPF 認証の有効化（Enable OSPF Authentication）	[一般パラメータ（General Parameters）] タブの **[ルーティング プロトコル（Routing Protocol）]** で **ospf** を選択した場合、 このフィールドは編集可能になります。 OSPF 認証を有効にする場合、このチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、**[OSPF 認証キー ID（OSPF Authentication Key ID）]** および **[OSPF 認証キー（OSPF Authentication Key）]** フィールドが有効になります。

フィールド	説明
OSPF 認証キー ID（OSPF Authentication Key ID）	このフィールドは、次の条件で編集可能になります。 ・[一般パラメータ（General タブの **[ルーティング プロトコル（Routing Protocol）]** フィールドで **ospf** を選択した場合。 ・上記の **[OSPF 認証の有効化（Enable OSPF Authentication）]** フィールドを有効にした場合。 キー **ID** が入力されます。
OSPF 認証キー（OSPF Authentication Key）	このフィールドは、次の条件で編集可能になります。 ・[一般パラメータ（General タブの [ルーティングプロトコル（Routing Protocol）] フィールドで **ospf** を選択した場合。 ・上記の **[OSPF 認証の有効化（Enable OSPF Authentication）]** フィールドを有効にした場合。 OSPF 認証キーは、スイッチからの 3DES キーである必要があります。注：プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。詳細については、「*認証キーの取得*」の項を参照してください。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

セキュリティ

[セキュリティ（Security）] タブは次のテーブルで説明されています。

データ センター インターコネクト（DCI） MACsec の設定の詳細については、「 Connecting Two

Fabrics with MACsec Using QKD」を参照してください。

フィールド	説明
DCI MACsec の有効化	DCI リンクで MACsec を有効にするには、このチェックボックスをオンにします。
QKD の有効化	暗号化用の量子キーを生成するために QKD サーバを有効にするには、このチェックボックスをオンにします。 **[QKD** を有効にする（**Enable QKD**）] オプションを有効にしないことにした場合、NDFC はキーを生成するための QKD サーバーを使用する代わりに ユーザーが指定した事前共有したキーを使用します。 [QKD を有効にする（ **Enable QKD** ）] オプションを無効にすると、 QKD に関連するすべてのフィールドが グレー表示されます。

フィールド	説明
DCI MACsec 暗号スイート	MACsec ポリシーの次の MACsec 暗号スイートのいずれかを選択します。 ・ **GCM-AES-128** ・ **GCM-AES-256** ・ **GCM-AES-XPN-128** ・ **GCM-AES-XPN-256** デフォルト値は **GCM-AES-XPN-256** です。
DCI MACsec プライマリキー文字列	プライマリ DCI MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。**AES_256_CMAC** の場合、キー文字列の長さは 130、**AES_128_CMAC** の場合、キー文字列の長さは 66. これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。 デフォルトのキー ライフタイムは無期限です。
DCI MACsec プライマリ暗号化アルゴリズム	プライマリ キー文字列に使用する暗号化アルゴリズムを選択します。**AES_128_CMAC** または **AES_256_CMAC** です。デフォルト値は **AES_128_CMAC** です。 プライマリ セッションが失敗した場合にバックアップ セッションを開始するように、デバイスのフォールバック キーを設定できます。
DCI MACsec フォールバック キー文字列	フォールバック MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。**AES_256_CMAC** の場合、キー文字列の長さは 130、**AES_128_CMAC** の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。 **[QKD の有効化（Enable QKD）]**オプションが選択されていない場合 、 この パラメータ は必須です。
DCI MACsec フォールバック暗号化アルゴリズム	フォールバック キー文字列に使用する暗号化アルゴリズムを選択します。**AES_128_CMAC** または **AES_256_CMAC** です。デフォルト値は **AES_128_CMAC** です。
QKD プロファイル名	暗号プロファイル名を指定します。 最大サイズは 63 です。
KME サーバー IP	キー管理エンティティ（KME）サーバの IPv4 アドレスを指定します。
KME サーバ ポート番号	KME サーバが使用するポート番号を指定します。
トラストポイント ラベル	認証タイプのトラストポイント ラベルを指定します。 最大サイズは 64 です。
証明書を無視する	着信証明書の検証をスキップするには、このチェックボックスをオンにしま

	す。

フィールド	説明
MACsec ステータス レポート タイマー	MACsec 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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[**保存（**Save**）**]** をクリックします。

高度

次のテーブルに**[**詳細（**Advanced**）**]** タブのフィールドが説明されています。すべてのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
VRF テンプレート（**VRF Template**）	VRF 作成のための VRF テンプレートを指定します。これらは、NDFC で提供される VRF 用の事前作成されたベスト プラクティス テンプレートです。テンプレートを指定する必要はありませんが、いずれかが自動的に選択されます。
ネットワークテンプレート（**Network Template**）	ネットワーク VRF 作成のための VRF テンプレートを指定します。これらは、NDFC で提供されるネットワーク用の事前作成されたベスト プラクティス テンプレートです。テンプレートを指定する必要はありませんが、いずれかが自動的に選択されます。
レイヤ **2** ホスト インターフェイス **MTU**	レイヤ 2 ホスト インターフェイスに MTU を指定します。この値は偶数にする必要があります。
デフォルトでのホスト インターフェイスのシャットダウン解除（**Unshut Host Interfaces by Default**）	デフォルトでホスト インターフェイスのシャットダウンを解除するには、このチェックボックスをオンにします。
電源モード	適切な電源モードを選択します。
CoPP プロファイル	ファブリックの適切なコントロール プレーン ポリシング（CoPP）プロファイル ポリシーを選択します。デフォルトでは、strict オプションが入力されます。

フィールド	説明
ブラウンフィールド ネットワーク名のフォーマット（**Brownfield Network Name Format**）	ブラウンフィールドのインポートまたは移行時にオーバーレイ ネットワーク名を作成するために使用するフォーマットを入力します。ネットワーク名には、アンダースコア（_）およびハイフン（-）以外の特殊文字または空白が含まれないようにしてください。ブラウンフィールドの移行が開始されたら、ネットワーク名を変更しないでください。ネットワーク名の命名規則については、「スタンドアロン ファブリックのネットワークの作成」の項を参照してください。 構文は [<string> | VLAN_ID] で、デフォルト値は **Auto_Net_VLANVLAN_ID** です。ネットワークを作成すると、指定した構文に従って名前が生成されます。 次のリストで構文内の変数について説明します。 ・**VLAN_ID**：ネットワークに関連付けられた VLAN ID を指定します。 VLAN ID はスイッチに固有であるため、 Nexus Dashboard Fabric Controller は、ネットワークが検出されたスイッチの 1 つから VLAN ID をランダムに選択し、名前に使用します。 VLAN ID がファブリック全体で一貫していない限り、これを使用しないことを推奨します。 ・**<string>**：この変数はオプションであり、ネットワーク名のガイドラインを満たす任意の数の英数字を入力できます。 オーバーレイ ネットワーク名の例は、Site_VLAN1234 です。 グリーンフィールド展開では、このフィールドを無視します。
ブートストラップ スイッチの CDP の有効化（**Enable CDP for Bootstrapped Switch**）	ブートストラップ スイッチの管理（mgmt0）インターフェイスで CDP を有効にします。デフォルトでは、ブートストラップ スイッチの場合、mgmt0 インターフェイスで CDP は無効にされています。
テナント **DHCP** の有効化（**Enable Tenant DHCP**）	機能 dhcp および関連する構成をファブリック内のすべてのスイッチでグローバルに有効にするには、このチェックボックスをオンにします。これは、テナント VRF の一部であるオーバーレイ ネットワークの DHCP をサポートするための前提条件です。 オーバーレイ プロファイルで **DHCP** 関連のパラメータを有効にする前に、[テナント **DHCP** の有効化（Enable Tenant DHCP）]が有効であることを確認します。
NX-API を有効化（**Enable NX-API**）	HTTPS での NX-API の有効化を指定します。
NX-API HTTPS ポート 数量	**[NX-API** の有効化（**Enable NX-API**）**]** オプションが有効になっている場合、フィールドがアクティブになります。 NX-API HTTPS ポート番号を入力します。デフォルト値は 443 です。

フィールド	説明
HTTP NX-API を有効化	HTTP での NX-API の有効化を指定します。HTTP を使用するには、**[NX-API** の有効化（**Enable NX-API**）] チェック ボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4 ~ レイヤ 7 サービス（L4～L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco Nexus Dashboard Fabric Controller がサポートするアプリケーションは、HTTP ではなく HTTPS を使用するようになります。 [NX-API の有効化（Enable NX-API）] チェックボックスをオンにし、**[HTTP** での **NX-API** の有効化（**Enable NX-API on HTTP**）] チェックボックスをオンにすると、アプリケーションは HTTP を使用します。
NX-API HTTP ポート 数量	**[HTTP NX-API** の有効化（**Enable HTTP NX-API**）] オプションが有効になっている場合、フィールドがアクティブになります。NX-API HTTPS ポート番号を入力します。デフォルト値は 80 です。
厳密な構成コンプライアンスの有効化	このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。これにより、双方向のコンプライアンス チェックが有効になり、インテント/期待されている構成に存在せず、実行構成内で追加された構成には、フラグが付けられます。デフォルトでは、この機能は無効になっています。
AAA **IP** 認証の有効化	IP 認証がリモート認証サーバーで有効になっている場合に、AAA IP 認証を有効にします。これは、スイッチにアクセスできる IP アドレスを顧客が厳密に制御できるシナリオで Nexus Dashboard Fabric Controller をサポートするために必要です。
トラップ ホストとしての **NDFC** の有効化	SNMP トラップの宛先として Nexus ダッシュボード ファブリック コントローラを有効にするには、このチェックボックスをオンにします。通常、ネイティブ HA Nexus ダッシュボードファブリックコントローラの導入では、eth1 VIP IP アドレスがスイッチの SNMP トラップ宛先として設定されます。デフォルトでは、このチェックボックスは有効になっています。
集約/アクセス自動ペアリングの有効化（**Enable Agg/Access Auto Pairing**）	back-to-back vPC の場合、トポロジに基づいて集約デバイスとアクセス デバイスを自動的にペアリングするには、このオプションを有効にします。
ルートマップ **fabric-rmap-redist-subnet** の作成（**Create Route-map fabric-rmap-redist- subnet**）	ルートマップ fabric-rmap-redist-subnet を作成するには、このオプションを有効にします。このルートマップはタグ 12345 とマッチします。
グリーンフィールド クリーンアップ オプション（**Greenfield Cleanup Option**）	PreserveConfig=no の場合、リロードせずにスイッチ設定を消去するには、このフィールドを有効にします。 有効なオプションは、[有効（Enable）] または [無効（Disable）] です。
集約自由形式設定（**Aggregation Freeform Config**）	show running configuration からキャプチャされたすべての集約デバイスの追加 CLI です。
フリーフォーム設定へのアクセス（**Access Freeform Config**）	show running configuration からキャプチャされたすべてのアクセス デバイスの追加 CLI です。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら［保存（Save）］をクリックします。

リソース

[リソース（**Resources**）**]** タブのフィールドについては、次の表で説明します。ほとんどのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
ネットワーク **VLAN** 範囲（**Network VLAN Range**）	スイッチごとのオーバーレイ ネットワークの VLAN 範囲（最小：2、最大：4094）。
Aggregation-Core/Aggregation-Edge 接続（**Aggregation-Core/Aggregation-Edge Connectivity**）	VRF Lite Aggregation-Core および Aggregation-Edge Router Inter-Fabric 接続のオプションを指定します。オプションは、次のとおりです。 ・自動（**Auto**）：アグリゲーションおよびコア スイッチで VRF Lite 設定を自動的に生成します。このオプションは、コア レイヤに Cisco Nexus 7000 または 9000 シリーズ スイッチを使用している場合にのみ適用されます。 ・手動（**Manual**）：コアレイヤに Cisco Catalyst 9000 シリーズ スイッチまたは Cisco ASR 9000 シリーズ アグリゲーション サービス ルータを使用している場合は、このフィールドで **[**手動（**Manual**）**]** を選択します。NDFC を通じて提供される必要なポリシーを使用して、ポリシーを手動で作成する必要があります。詳細については、VRF Lite を参照してください。
VRF-Lite サブインターフェイス **dot1q** 範囲（**VRF-Lite Subinterface dot1q Range**）	VRF Lite 接続の集約 dot1q 範囲ごとに指定します（最小：2、最大：4093）。
集約とコア**/**エッジ での 自動生成 **VRF** ライト構成	集約およびコア/エッジデバイスでの VRF Lite サブインターフェイスとピアリング設定の自動生成を制御するオプションです。このオプションを有効にすると、自動的に作成された VRF Lite リンクで［フラグの自動生成（Auto Generate Flag）］が有効になります。
VRF Lite IP バージョン（**VRF Lite IP Version**）	VRF Lite の IP バージョンを選択します。オプションは次のとおりです。 ・**IPv4_only** ・**IPv6_only** ・**IPv4_and_IPv6**
IPv4 VRF サブネット **IP** 範囲と **IPv4 VRF** サブネット マスク長（**IPv4 VRF Subnet IP Range and IPv4 VRF Subnet Mask Length**）	ピアツーピア集約コア接続、および vPC 集約スイッチ間のピアリングを割り当てる IPv4 アドレス範囲。 必要に応じて、次のフィールドを更新します。画面に表示される値は自動的に生成されます。 IP アドレス範囲または VRF/ネットワーク VLAN 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、レイヤ 2 およびレイヤ 3 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）］をクリックして保存します。

フィールド	説明
IPv6 VRF サブネット **IP** 範囲と **IPv6 VRF** サブネット マスク長（**IPv6 VRF Subnet IP Range and IPv6 VRF Subnet Mask Length**）	ピアツーピア集約コア接続、および vPC 集約スイッチ間のピアリングを割り当てる IPv6 アドレス範囲。 必要に応じて、次のフィールドを更新します。画面に表示される値は自動的に生成されます。IP アドレス範囲または VRF/ネットワーク VLAN 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、レイヤ 2 およびレイヤ 3 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）] をクリックして保存します。
VRF Lite VLAN 範囲（**VRF Lite VLAN Range**）	集約ペア間の VRF ごとの SVI ピアリングの VLAN 範囲（最小：2、最大：4094）。
特定の **vPC/**ポート チャネル識別子範囲の活用	リーフ-ToR スイッチペアリングの vPC 識別子のカスタム範囲を指定します。最小許容値は 1、最大許容値は 4099 です。
vPC/ポート チャネル 識別子範囲	リーフ ToR スイッチペアリングの vPC 識別子を自動割り当てするためのカスタム vPC 識別子範囲を指定します。最小許容値は 1、最大許容値は 4099 です。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[**保存（**Save**）**]** をクリックします。

管理性

次の表では、**[**管理性（**Manageability**）**]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
DNS サーバー **IP**（**DNS Server IPs**）	DNS サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。
DNS サーバー **VRF**（**DNS Server VRFs**）	すべての DNS サーバに 1 つの VRF を指定するか、DNS サーバーごとに 1 つの VRF を指定します。
NTP サーバー **IP**（**NTP Server IPs**）	NTP サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。
NTP サーバー **VRF**（**NTP Server VRFs**）	すべての NTP サーバーに 1 つの VRF を指定するか、NTP サーバーごとに 1 つの VRF を指定します。
Syslog サーバー **IP**（**Syslog Server IPs**）	syslog サーバーの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

Syslog サーバーの重要度（**Syslog Server Severity**）	syslog サーバーごとに 1 つの syslog 重大度値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。
フィールド	説明
Syslog サーバー **VRF**（**Syslog Server VRFs**）	すべての syslog サーバーに 1 つの VRF を指定するか、syslog サーバーごとに 1 つの VRF を指定します。
AAA フリーフォーム構成（**AAA Freeform Config**）	AAA フリーフォーム構成を指定します。 ファブリック設定で AAA 構成が指定されている場合は、ソースが **UNDERLAY_AAA**、説明が **AAAConfigurations** である **switch_freeform** PTI が作成されます。
バナー	Day バナーのメッセージを指定します。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら［保存（Save）］をクリックします。

ブートストラップ

次の表では、**[**ブートストラップ（**Bootstrap**）**]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
ブートストラップの有効化	ブートストラップ機能を有効にします。ブートストラップを使用すると、新しいデバイスを day-0 段階で簡単にインポートし、既存のファブリックに組み込むことができます。ブートストラップは NX-OS POAP 機能を活用します。 スイッチを追加し、POAP 機能を使用するには、**[**ブートストラップの有効化（**Enable Bootstrap**）**]** と **[**ローカル **DHCP** サーバの有効化（**Enable Local DHCP Server**）**]** のチェックボックスをオンにします。 ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。 ・外部 DHCP サーバー：**[**スイッチ管理デフォルト ゲートウェイ（**Switch Mgmt Default Gateway**）**]** および **[**スイッチ管理 **IP** サブネット プレフィックス（**Switch Mgmt IP Subnet Prefix**）**]** フィールドに外部 DHCP サーバーに関する情報を入力します。 ・[ローカル DHCP サーバー（Local DHCP Server）]：**[**ローカル **DHCP** サーバー（**Local DHCP Server**）**]** チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

ローカル **DHCP** サーバーの有効化（**Enable Local DHCP Server**）	ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP** スコープ開始アドレス（**DHCP Scope Start Address**）**]** および **[DHCP** スコープ終了アドレス（**DHCP Scope End Address**）**]** フィールドが編集可能になります。 このチェックボックスをオンにしない場合、Nexus ダッシュボード ファブリック コントローラは自動 IP アドレス割り当てにリモートまたは外部 DHCP サーバを使用します。
フィールド	説明
DHCP バージョン	このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[**スイッチ管理 **IPv6** サブネット プレフィックス（**Switch Mgmt IPv6 Subnet Prefix**）**]** フィールドは無効になります。DHCPv6 を選択すると、**[**スイッチ管理 **IP** サブネット プレフィックス（**Switch Mgmt IP Subnet Prefix**）**]** は無効になります。 Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチがレイヤー 2 隣接 (eth1 またはアウトオブバンド サブネットが /64 である必要があります) であるか、または IPv6 /64 サブネット内に存在してレイヤー 3 隣接である場合にのみ、IPv6 POAP をサポートします。 /64 以外のサブネット プレフィックスはサポートされません。
DHCP スコープ開始アドレス（**DHCP Scope Start Address**）と **DHCP** スコープ終了アドレス（**DHCP Scope End Address**）	スイッチ アウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。
スイッチ管理デフォルトゲートウェイ（**Switch Mgmt Default Gateway**）	スイッチの管理 VRF のデフォルト ゲートウェイを指定します。
スイッチ　管理 **IP** サブネット プレフィックス（**Switch Mgmt IP Subnet Prefix**）	スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ~ 30 の間である必要があります。 *DHCP スコープおよび管理デフォルト ゲートウェイ IP アドレスの仕様*：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ~ 10.0.1.254 の範囲内であることを確認してください。
DHCPv4 マルチ サブネット範囲（**DHCPv4 Multi Subnet Scope**）	1 行に 1 つのサブネット範囲を入力して、フィールドを指定します。**[**ローカル **DHCP** サーバーの有効化（**Enable Local DHCP Server**）**]** チェックボックスをオンにすると、このフィールドは編集可能になります。範囲のフォーマットは次のように定義します。 **[DHCP** スコープ開始アドレス、**DHCP** スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（**DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix**）**]**

	例：10.6.0.2、10.6.0.9、16.0.0.1、24
AAA 構成の有効化（**Enable AAA Config**）	ブートストラップ後のデバイス起動構成の一部として [管理可能性（Manageability）] タブから AAA 構成を含めるには、このチェックボックスをオンにします。
ブートストラップ フリーフォーム構成（**Bootstrap Freeform Config**）	（オプション）必要に応じて追加のコマンドを入力します。たとえば、デバイスにプッシュするいくつかの追加の設定が必要であり、ポスト デバイス ブートストラップが使用可能である場合、このフィールドでキャプチャして要求のとおりに保存することが可能です。デバイスの起動後、**[**ブートストラップ フリーフォームの設定（**Bootstrap Freeform Config**）**]** フィールドで定義された設定を含めることができます。 running-config をコピーして **[**フリーフォームの設定（**freeform config**）**]** フィールドに、NX-OS スイッチの実行設定に示されているように、正しいインデントでコピーアンドペーストします。freeform config は running config と一致する必要があります。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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[**保存（**Save**）**]** をクリックします。

コンフィギュレーションのバックアップ

次の表では、**[**構成バックアップ（**Configuration Backup**）**]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベストプラクティスの構成に基づいて自動的に入力されますが、必要に応じてフィールドを更新できます。

フィールド	説明
毎時ファブリック バックアップ	ファブリック構成とインテントの毎時バックアップを有効にします。時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。
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。
予定時刻	スケジュールされたバックアップ時間を 24 時間フォーマットで指定します。**[**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。 スケジュールされたバックアップは、指定した時刻に最大 2 分の遅延でトリガーされます。スケジュールされたバックアップは、構成の展開ステータスに関係なくトリガーされます。 NDFC で保持されるファブリック バックアップの数は、**[**管理（**Admin**）**] > [**システム設定（**System Settings**）**] > [**サーバー設定（**Server Settings**）**] > [LAN** ファブリック（**LAN Fabric**）**] > [**ファブリックあたりの最大バックアップ数（**Maximum Backups per Fabric**）**]** によって決定されます。 保持できるアーカイブ ファイルの数は、**[**サーバー プロパティ（**Server Properties**）**]** ウィンドウの **[**保持するデバイスあたりのアーカイブ ファイル数（**# Number of archived files per device to be retained:**）**]** フィールドで設定します。 即時バックアップをトリガするには、次の手順を実行します。 1. **[**概要（**Overview**）**] > [**トポロジ（**Topology**）**]** を選択します。 2. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。 3. ファブリック内のスイッチを右クリックし、**[**構成のプレビュー（**Preview Config**）**]** を選択します。 4. このファブリックの **[**構成のプレビュー（**Preview Config**）**]** ウィンドウで、**[**すべて再同期（**Re-Sync All**）**]** をクリックします。 ファブリック トポロジ ページでファブリック バックアップを開始することもできます。クリックします。 [アクション（Actions）] ペインで [今すぐバックアップ（Backup Now）] をクリックします。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら［保存（Save）］をクリックします。

Flow Monitor

次の表では、**[**フローモニター（**Flow Monitor**）**]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、

必要に応じてフィールドを更新できます。

フィールド	説明
NetFlow を有効にする	このファブリックの集約デバイスで NetFlow を有効にするには、このチェックボックスをオンにします。デフォルトでは、Netflow は無効になっています。有効にすると、NetFlow 構成は、NetFlow をサポートするすべての集約デバイスに適用されます。 ファブリックで NetFlow が有効になっている場合でも、ダミーの no_netflow PTI を設定することにより、特定のスイッチで netflow を処理しないようにすることができます。 netflow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または VRF レベルで netflow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の NetFlow サポートの詳細については、Understanding LAN Fabrics の「Netflow Support」の項を参照してください。

[ネットフロー エクスポータ（Netflow Exporter）**]** エリアで、**[**アクション（**Actions**）**] > [**追加（Add）**]** の順にクリックして、1 つ以上の Netflow エクスポータを追加します。このエクスポータは、NetFlow データの受信側です。この画面のフィールドは次のとおりです。

フィールド	説明
[エクスポータ名（**Exporter Name**）**]**	エクスポータの名前を指定します。
IP	エクスポータの IP アドレスを指定します。
VRF	エクスポータがルーティングされる VRF を指定します。
送信元インターフェイス	送信元インターフェイス名を入力します。
UDP ポート	NetFlow データがエクスポートされる UDP ポートを指定します。

[保存（**Save**）**]** をクリックしてエクスポータを構成します。破棄するには、**[**キャンセル（**Cancel**）**]** をクリックします。既存のエクスポータを選択し、**[**アクション（**Actions**）**] > [**編集（**Edit**）**]** または **[**アクション（**Actions**）**] > [**削除（**Delete**）**]** を選択して、関連するアクションを実行することもできます。

[Netflow レコード（**Netflow Record**）**]** 領域で、**[**アクション（**Actions**）**] > [**追加（**Add**）**]** の順にクリックして、1 つ以上の Netflow レコードを追加します。この画面のフィールドは次のとおりです。

フィールド	説明
レコード名	レコードの名前を指定します。
レコード テンプレート	レコードのテンプレートを指定します。レコード テンプレート名の 1 つを入力します。

次の 2 つのレコード テンプレートを使用できます。カスタム Netflow レコード テンプレートを作成できます。テンプレート ライブラリに保存されているカスタム レコード テンプレートは、ここで使用できます。

- **[netflow_ipv4_record]** : IPv4 レコード テンプレートを使用します。
- netflow_l2_record **-** レイヤ **2** レコード テンプレートを使用します。
  - [レイヤ 2 レコード（Is Layer2 Record）]：レコードが **Layer2 Netflow** の場合は、このチェックボックスをオンにします。

[保存（**Save**）**]** をクリックしてレポートを構成します。**[**キャンセル（**Cancel**）**]** をクリックして破棄します。既存のレコードを選択し、**[**アクション（**Actions**）**] > [**編集（**Edit**）**]** または **[**アクション（**Actions**）**] > [**削除（**Delete**）**]** を選択して、関連するアクションを実行することもできます。

[Netflow モニター（**Netflow Monitor**）**]** 領域で、**[**アクション（**Actions**）**] > [**追加（**Add**）**]** の順にクリックして、1 つ以上の Netflow モニターを追加します。この画面のフィールドは次のとおりです。

フィールド	説明
モニター名	モニターの名前を指定します。
レコード名	モニターのレコードの名前を指定します。
エクスポータ **1** の名前	NetFlow モニターのエクスポータの名前を指定します。
エクスポータ **2** 名（オプション）。	NetFlow モニターのセカンダリ エクスポータの名前を指定します。

各 NetFlow モニターで参照されるレコード名とエクスポータは、**[Netflow** レコード（**Netflow Record**）**]** と **[Netflow** エクスポータ（**Netflow Exporter**）**]** で定義する必要があります。

[Netflow サンプラー（Netflow Sampler）**]** エリアで、**[**アクション（**Actions**）**] > [**追加（**Add**）**]** の順にクリックして、1 つ以上の Netflow サンプラーを追加します。これらはオプションのフィールドであり、ファブリックに N7K アグリゲーション スイッチがある場合にのみ適用されます。この画面のフィールドは次のとおりです。

フィールド	説明
サンプラー名	サンプラーの名前を指定します。
サンプル数	サンプル数を指定します。
サンプリングごとのパケット数。	サンプリングごとのパケット数を指定します。

[保存（**Save**）**]** をクリックして、モニターを構成します。破棄するには **[**キャンセル（**Cancel**）**]** をクリックします。既存のモニタを選択し、**[**アクション（**Actions**）**] > [**編集（**Edit**）**]** または **[**アクション（**Actions**）**] > [**削除（**Delete**）**]** を選択して、関連するアクションを実行することもできます。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら［保存（Save）］をクリックします。

拡張クラシック LAN ファブリックでの集約とアクセスのペアリングについて

NDFC 12.1.3 リリースでは、最適なトラフィック エンジニアリングのために集約スイッチとアクセス スイッチを自動的に検出してペアリングするワンクリック vPC 機能が NDFC に追加されました。デフォルトでは、自動集約アクセス ペアリング オプションが有効になっています。つまり、 再計算して展開操作を実行すると 、NDFC は集約とアクセス スイッチ間の接続を自動的に検出し、検出されたサポートされているトポロジに基づいて適切な設定を生成します。設定には、NDFC がペアリングされた集約スイッチとアクセス スイッチに自動的にプッシュする vPC ドメインが含まれます。これらの集約アクセス ペア間のリンクは、共通の vPC 論理的な構造にバンドルされます。

NDFC アグリゲーションとアクセスのペアリングの詳細については、『Enhanced Classic LAN in Cisco Nexus Dashboard Fabric Controller (NDFC) Release 12.1.3』 ホワイトペーパーを参照してください。

集約とアクセスのペアリングを設定するためのワークフロー

1. 拡張クラシック LAN ファブリックの作成詳細については、「拡張クラシックの作成 」を参照してください。
2. ファブリックで検出されたスイッチを表示します。詳細については、LAN 動作モードのスイッチの追加の「ファブリックへのスイッチの追加」の項を参照してください。
3. ブートストラップを使用してスイッチを追加します。詳細については、『LAN 操作モードへのスイッチの追加』の「ブートストラップ メカニズムを使用したスイッチの追加」のセクションを参照してください。
4. 集約スイッチとアクセス スイッチのロールを定義します。詳細については、『LAN 動作モードのスイッチの追加』の「スイッチ ロールの割り当て」の項を参照してください。
5. vPC ペアリングを構成します。詳細については、『LAN 動作モードのスイッチの追加』の「vPC セットアップの作成 」の項を参照してください。
6. 再計算と展開を行います。

集約とアクセスのペアの作成

1. 集約スイッチとアクセス スイッチを設定するには、次の手順を実行します。集約スイッチはポート チャネルを介してアクセス スイッチに接続されます。
2. 集約およびアクセス スイッチを Enhanced Classic LAN ファブリックに追加し、スイッチのタイプに応じてロールを **[**アクセス（**Access**）**]** または **[**集約（**Aggregation**）**]** に設定します。

   拡張クラシック LAN ファブリックでは、NDFC は少なくとも 2 つの集約スイッチをサポートし、集約スイッチは vPC ペアにする必要があります。

3. **[**ファブリックの概要（**Fabric Overview**）**] > [**スイッチ（**Switches**）**]** ページで、集約スイッチを選択します。
4. **[**アクション（**Actions**）**] > [**アクセス ペアリング（**Access Pairing**）**]**をクリックします。

   [アクセス ペアリング（**Access Pairing**）**]** ページでは、上部に集約スイッチが表示され、集約スイッチの下にペアリング可能なアクセス スイッチのリストが表示されます。集約スイッチのステータスが **[** 詳 細 （ **Details** ） **]** 列 に デ ィ ス プ レ イ さ れ ま す 。

5. **[保存（Save）]** をクリックします。
6. **[ファブリックの概要（Fabric Overview）]** ページで、**[アクション（Actions）] > [再計算と展開（Recalculate and Deploy）]** をクリックします。
7. **[構成の展開（Deploy Configuration）]** ページで構成の展開が完了したら、**[閉じる（Close）]** をクリックします。

集約-アクセス スイッチのペア解除

1. **Enable <switch-name> Pairing as Access Pairing** チェックボックスをオンにして、スイッチのペアリングを解除します。

   オーバーレイが接続されている場合は、集約アクセスペアのペアを解除できません。

2. **[ファブリックの概要（Fabric Overview）]** ページで、**[アクション（Actions）] > [再計算して展開（Recalculate and Deploy）]** の順にクリックして、ペアリング解除操作を完了します。

集約アクセス ペアリングの特定の vPC/ポート チャネル識別子範囲の構成

この機能を使用すると、次のことが可能になります。

- **[特定の vPC/ポートチャネル ID 範囲を使用（Use Specific vPC/Port-Channel ID Range）]** フィールドを有効にして、集約アクセスペアリングの特定の vPC/ポートチャネル識別子範囲を設定します。NDFC は、 **vPC/ポートチャネル識別子範囲** フィールドに、推奨される vPC/ポートチャネル識別子範囲を表示します。
- ペア編集されたスイッチの vPC/ポートチャネル識別子を編集するには、**[アクセス ペアリング]** ページで [アクション（Action）] > [ペアリングの編集（Edit Pairing）] をクリックします。

集約アクセス ペアリングの vPC/ポート チャネル識別子範囲を指定するためのファブリック設定

1. 拡張クラシック **LAN** ファブリックの **[ファブリック概要（Fabric Overview）]** ページに戻ります。詳細については、「拡張クラシック LAN ファブリックの作成」を参照してください。
2. **[vPC]** タブをクリックします。
3. [特定の vPC/ポートチャネル ID 範囲を使用（**Use Specific vPC/Port-Channel ID Range**）] チェックボックスをオンにして、集約とアクセスのペアリングに特定の vPC/ポートチャンネル識別子範囲を使用します。

   [vPC/ポートチャネル ID 範囲（vPC/Port-Channel ID Range）] フィールドに

   推奨値が表示されます。推奨値は 1 ~ 499 です。

   値がなくなった場合は、既存の範囲を増やすか、範囲を追加ます 。
4. 推奨値を使用しない場合は、**[vPC/Port-Channel ID Range]** フィールドに範囲を指定します。
5. **[保存（Save）]** をクリックします。

   新しい範囲は、新しいペアリングに適用されます。

集約またはアクセス vPC/ポート チャネル ID の編集

1. **[ファブリックの概要（Fabric Overview）] > [スイッチ（Switches）]** ページで、編集する集約スイッチを選択し、 **[アクション（Actions）] > [アクセス ペアリング（Access Pairing）]** をクリックします。

   [アクセス ペアリング（Access Pairing）] ページが表示され、ペアリングされた集約スイッチの水平バーが表示されます。
2. **[アクション（Action）]** 列の **[ペアリングの編集（Edit Pairing）]** をクリックします。

   アクセス-集約のペアになったスイッチのページが表示されます。

   自動集約-アクセス ペアリングのために、[**Enable <switch-name> Pairing as Access Pairing**]チェックボックスがオンになっています。

3. ページの右側の列にある矢印をクリックして、フィールドを表示します。
4. 値を変更する場合は、アクセスまたは集約 vPC/ポート チャネル ID を変更します。
5. **[**保存（**Save**）**]** をクリックします。

ペアリングされたスイッチにオーバーレイが接続されている場合、vPC/ポート チャネル ID を変更することはできません。

6. **[**ファブリックの概要（**Fabric Overview**）**] > [**スイッチ（**Switches**）**]** ページで、**[**アクション（**Actions**）**] > [**再計算と展開（**Recalculate and Deploy**）**]** をクリックします。**[**構成の展開（**Deploy Configuration**）**]**ページが表示され、集約スイッチのリストが示されます。

展開が成功すると、[ファブリックステータス（ **Fabric Status** ）] 列に [同期中（**In-Sync**）] と表示されます。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。