



拡張拡張クラシック LAN、リリース
12.1.3

目次

新機能と更新情報.....	1
拡張クラシック LAN ファブリックの作成.....	2
一般的なパラメータ.....	3
スパニングツリー.....	3
VPC.....	5
プロトコル.....	5
高度.....	8
リソース.....	12
管理性.....	13
ブートストラップ.....	14
構成 バックアップ.....	17
Flow Monitor.....	18
著作権.....	21

新機能と更新情報

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 12.1.3	再編成されたコンテンツ	このドキュメント内のコンテンツは元来 『Cisco NDFC-Fabric Controller 構成ガイド』 または 『Cisco NDFC-SAN Controller 構成ガイド』 で提供されました。 リリース 12.1.3 以降、このコンテンツは現在、このドキュメントでのみ提供されており、これらのドキュメントでは提供されなくなっています。

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：

[ローカルエリアネットワーク (LAN)] > **[ファブリック (Fabric)]**

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](#)
- [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。 <ul style="list-style-type: none">• 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。 <ul style="list-style-type: none">• 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	[ルーティングプロトコル (Routing Protocol)] で ebgp を選択した場合、このフィールドは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 (Enable Performance 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。

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)	<p>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。</p> <ul style="list-style-type: none"> • 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 <p> スパニングツリー設定とブリッジ設定は、集約レイヤのみで適用できます。</p>
スパニングツリー VLAN 範囲 (Spanning Tree VLAN Range)	<p>VLAN 範囲を指定します。例 :</p> <p>1, 3-5, 7, 9-11</p> <p>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。</p>
MST インスタンス範囲 (MST Instance Range)	<p>MST インスタンス範囲を指定します。例 : 0-</p> <p>3,5,7-9</p> <p>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。</p>
スパニング ツリー ブリッジ優先度 (Spanning Tree Bridge Priority)	<p>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。</p>
スパニングツリー Hello 間隔 (Spanning Tree Hello Interval)	<p>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。</p> <p>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。</p>
スパニング ツリー 転送遅延 (Delay SpanningTree Forward Delay)	<p>転送遅延タイマーを秒数で設定します。</p> <p>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。</p>
スパニング ツリー 最 大エイジング間隔 (Spanning Tree Max Age Interval)	<p>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。</p> <p>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。</p>
スパニング ツリー パスコスト方式 (SpanningTree Pathcost Method)	<p>オプションは次のとおりです。</p> <ul style="list-style-type: none"> • 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。 <p>集約デバイスにのみ適用されます。</p>

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が自動的に Cisco が推奨するベストプラクティスの構成に基づいて入力されますが、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。 <ul style="list-style-type: none">• 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。 <ul style="list-style-type: none">• 最小値 : 1• 最大値 : 3600
vPC ピア リンク ポート チャンネル ID (vPC Peer Link Port Channel ID)	vPC ピア リンクのポートチャンネル 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。 <ul style="list-style-type: none">• 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)	<p>[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。</p> <p>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。</p>
フィールド	説明
OSPFエリアID	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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 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。 <p>IP アドレス フォーマットの OSPF エリア ID。</p>
OSPFv3 プロセス タグ (OSPFv3 Process Tag)	<p>[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。</p> <p>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。</p>
OSPFv3 エリア ID (OSPFv3 Area ID)	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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 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。 <p>OSPFv3 エリア ID (OSPFv3 Area ID) は IP アドレス フォーマットです。</p>
BGP の有効化 (Enable BGP) 認証	<p>[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 ebgp を選択した場合、このフィールドは編集可能になります。</p> <p>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。</p>



BGP パスワード キー暗号化タイプ (BGP Password Key Encryption Type)	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p>
BGP ネイバーパスワード (BGP Neighbor Password)	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p>
OSPF 認証の有効化 (Enable OSPF Authentication)	<p>[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。</p> <p>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 フィールドおよび OSPF 認証キー フィールドが有効になります。</p>
フィールド	説明
OSPF 認証キー ID (OSPF Authentication Key ID)	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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 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。 <p>キー ID が入力されます。</p>
OSPF 認証キー (OSPF Authentication Key)	<p>このフィールドは、次の条件で編集可能になります。</p> <ul style="list-style-type: none"> • [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 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。 <p>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。</p>

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 (Layer 2 Host Interface 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 (UnshutHost 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

<p>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)</p>	<p>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、スタンダアロン 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。</p> <p>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。</p> <p>次のリストで構文内の変数について説明します。</p> <ul style="list-style-type: none"> • VLAN_ID : ネットワークに関連付けられた VLAN ID を指定します。 <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • <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。 <p>オーバーレイ ネットワーク名の例は、Site_VLAN1234 です。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>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。</p> </div>
<p>ブートストラップスイッチの CDP の有効化 (Enable CDP for Bootstrapped Switch)</p>	<p>ブートストラップ スwitch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witchの場合、mgmt0 インターフェイスで CDP は無効にされています。</p>
<p>テナント DHCP の有効化 (Enable Tenant DHCP)</p>	<p>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。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>オーバーレイプロファイルの DHCP 関連パラメータを有効化する前に、</p> <p>[テナントDHCPの有効化 (Enable Tenant DHCP)] が有効になっていることを確認してください。</p> </div>

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	<p>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 の使用を開始します。</p> <p> [NX-API の有効化 (Enable NX-API)] チェックボックスをオンにし、</p> <p>[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。</p>
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 (Enable Strict Config Compliance)	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 (Enable AAA IP Authorization)	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 (Enable NDFC as Trap Host)	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)	バックツーバック 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。

ルートをマップ fabric-rmap-redist-subnet の作成 (Create Route-map fabric-rmap-redist-subnet)	ルートをマップ 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。このルートをマップはタグ 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)	<p>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。</p> <ul style="list-style-type: none"> • 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 およびコア/エッジでの VRF Lite 設定の自動生成 (Auto Generate VRF Lite Configuration on Aggregation and Core/Edge)	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)	<p>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。</p> <ul style="list-style-type: none"> • IPv4_only • IPv6_only • IPv4_and_IPv6

<p>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)</p>	<p>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。</p> <p>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。</p> <p>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。</p> <ol style="list-style-type: none"> 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。 保存します。
<p>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)</p>	<p>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。</p> <p>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。</p> <ol style="list-style-type: none"> 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。 保存します。
<p>VRF Lite VLAN 範囲 (VRF Lite VLAN Range)</p>	<p>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) 。</p>

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
<p>DNS サーバー IP (DNS Server IPs)</p>	<p>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。</p>

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。
フィールド	説明
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。
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 設定が指定されている場合は、 switch_freeform PTI で、ソースが UNDERLAY_AAA で説明が AAA Configurations であるものが作成されます。
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	<p>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。</p> <p>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 サーバーの有効化 (Enable Local DHCP Server)] のチェックボックスをオンにします。</p> <p>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。</p> <ul style="list-style-type: none"> 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。
フィールド	説明
ローカル DHCP サーバーの有効化 (Enable Local DHCP Server)	<p>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。</p> <p>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。</p>
DHCP バージョン	<p>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。</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 10px;"> <p> Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが レイヤ 2 隣接 (eth1 またはアウトオブバンドサブネットは /64 である必要があります) またはいずれかの IPv6/64 サブネットに存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。プレフィックスが /64 以外のサブネットはサポートされません。</p> </div>

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)	<p>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。</p> <p><i>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 (DHCP scope and management default gateway IP address specification) :</i> 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。</p>
DHCPv4 マルチサブネット範囲 (DHCPv4 Multi Subnet Scope)	<p>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。</p> <p>[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)]</p> <p>例 : 10.6.0.2, 10.6.0.9, 10.6.0.1, 24</p>
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。
フィールド	説明
ブートストラップ構成 自由形式	(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構成 (Bootstrap Freeform Config)] フィールドで定義された構成を含めることができます。

running-config をコピーして [フリーフォーム構成 (freeform config)] フィールドに、NX-OS スイッチの実行設定と同様の、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。

構成 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。

フィールド	説明
予定時刻	<p>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。</p> <p>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。</p> <p>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。</p> <p>NDFC で保持されるファブリック バックアップの数は、[設定 (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。</p> <p>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。</p> <p>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。</p> <ol style="list-style-type: none"> 1. [LAN]>[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。 <p>ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[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。</p>

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
NetFlow を有効にする	<p>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。</p> <p>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。</p> <p>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 サポートについては、Netflow Support を参照してください。</p>

[**ネットフロー エクスポート (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 エクスポートを追加します。このエクスポートは、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。

- [**エクスポート名 (Exporter Name)**] : エクスポートの名前を指定します。
- [**IP**] : エクスポートの IP アドレスを指定します。
- [**VRF**] : エクスポート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 (Source Interface)**] : **送信元インターフェイス名**を入力します。
- [**UDP ポート (UDP Port)**] : 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トを構成します。破棄するには、[**キャンセル (Cancel)**] をクリックします。既存のエクスポートを選択し、[**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 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 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。

- [**レコード名 (Record Name)**] : レコードの名前を指定します。
- [**レコードテンプレート (Record Template)**] : 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。破棄するには [**キャンセル (Cancel)**] をクリックします。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。

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。

- [**モニター名 (Monitor Name)**] : モニターの名前を指定します。
- [**レコード名 (Record Name)**] : モニターのレコードの名前を指定します。
- [**エクスポート 1 の名前 (Exporter1 Name)**] - ネットフロー モニタのエクスポートの名前を指定します。
- [**エクスポート 2 の名前 (Exporter2 Name)**] - (オプション) ネットフロー モニタの副次的なエクスポートの名前を指定します。

各 netflow モニタで参照されるレコード名とエクスポートは、「**Netflow レコード (Netflow Record)**」と「**Netflow エクスポート (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。

- [**サンプラー名 (Sampler Name)**] : サンプラーの名前を指定します。
- サンプル数
- サンプリングごとのパケット数。

[**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。

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』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco 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ー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。

シスコおよびシスコのロゴは、シスコ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。シスコの商標の一覧については、<http://www.cisco.com/go/trademarks> を参照してください。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シップ関係が存在することを意味するものではありません。(1110R)。

© 2017-2023 Cisco Systems, Inc. All rights reserved.