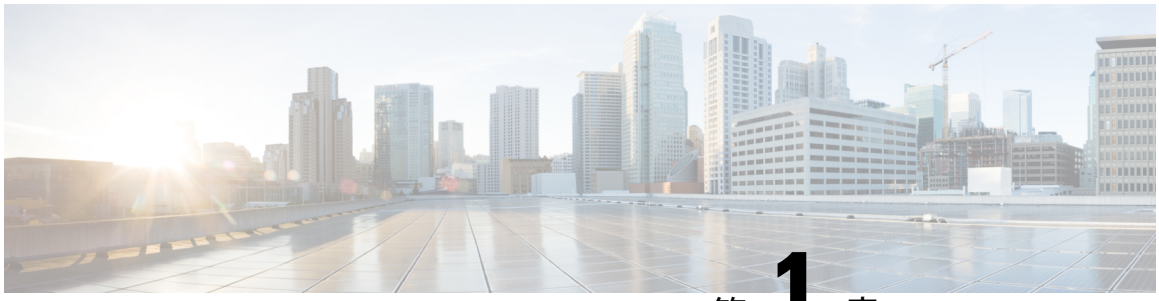
『Cisco NDFC SAN コントローラ 設定ガイド、リリース 12.0.x』

初版：2021 年 9 月 30 日

最終更新：2021 年 12 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

概要

Web UI を理解する

Cisco Nexusダッシュボード ファブリック コントローラ Web UIを初めて起動すると、**[機能管理（Feature Management）]** ウィンドウが開きます。展開タイプを選択すると、左側のペインにパーソナリティに関連するメニューが表示されます。

上部ペインには、次の UI 要素が表示されます。

- **[ホーム（Home）]** アイコン：クリックして Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **[Nexus ダッシュボード（Nexus Dashboard）]**：クリックして、Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **フィードバック**：Cisco Nexusダッシュボード ファブリック コントローラ に関するフィードバックを提供できます。この説明については、ユーザフィードバック （2 ページ） を参照してください。
- **[ヘルプ（Help）]**：**[ヘルプ（Help）]** をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
  - **Nexusダッシュボードについて**：Cisco Nexusダッシュボード ファブリック コントローラ が導入されているCisco Nexusダッシュボードのバージョンを表示します。
  - **ウェルカム画面**：最新情報を表示します。Web UI を起動するたびに、このページを表示するかどうかを選択できます。
  - **[ヘルプセンター（Help Center）]**：クリックすると、[ヘルプセンター（Help Center）] ページが表示されます。このページからさまざまな製品ドキュメントにアクセスできます。

ページの最後までスクロールして、Nexus Dashboard にインストールされているサービスを表示します。サービスをクリックして **[ヘルプセンター（Help Center）]** を表示します。

- **[ユーザーロール（User Role）]**：現在ログインしているユーザーのロール（**admin**など）が表示されます。ユーザー名をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
  - **[ユーザー設定（User Preferences）]**：ログインするたびにウェルカム画面を表示するかどうかを設定できます。
  - **[パスワードの変更（Change Password）]**：現在のログインユーザのパスワードを変更できます。

    ネットワーク管理者ユーザの場合、他のユーザのパスワードを変更できます。
  - **[ログアウト（Logout）]**：Web UI を終了し、ログイン画面に戻ります。
- **[Cisco Nexusダッシュボード ファブリック コントローラ Persona]**：展開ペルソナを指定します – **ファブリックコントローラ**、**SAN コントローラ**、または**ファブリック検出**。

UI の一般的なアイコン：

- **ハンバーガー** アイコン-ホーム画面の製品名の横にある**ハンバーガー** アイコンをクリックすれば、ホーム画面のメニュー項目を最小化することや、メニュー項目を詳細に表示することができます。
- **更新** アイコン：更新アイコンをクリックすると、画面が更新されます。

ユーザフィードバック

Cisco Nexusダッシュボード ファブリック コントローラ では、アプリケーションに関するフィードバックを提供できます。この機能を使用して、新しい機能/拡張機能を要求できます。要求は Cisco Nexusダッシュボード ファブリック コントローラ のマーケティング エンジニアに送信されます。エンジニアは要件を評価し、今後のリリースに機能または拡張機能を含めます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UIを使用してフィードバックを提供するには、次の手順を実行します。

手順

ステップ 1 **[フィードバック (Feedback)]** をクリックします。これはNexusダッシュボード ファブリック コントローラ アプリケーションの右上隅にあります。

これを初めて使用する場合は、Cisco Nexus ダッシュボードで DNS とプロキシ サーバーを設定する必要があります。

ステップ 2 接続を確立するには、ブラウザで **[Cisco Nexus ダッシュボード (Cisco Nexus Dashboard)]** に移動し、次の手順を実行します。

a) Cisco Nexus ダッシュボードの Web UIで、**[インフラストラクチャ (Infrastructure)]** > **[クラスタ設定 (Cluster Configuration)]** を選択します。

[クラスタ設定全般 (Cluster Configuration General)] タブが表示されます。

b) **[プロキシ設定 (Proxy Configuration)]** 領域で、**[編集 (Edit)]** アイコンをクリックします。

c) **[サーバー (Servers)]** 領域で、**[サーバーの追加 (Add Server)]** をクリックします。

d) プロトコルのタイプとして、**[HTTP]** または **[HTTPS]** を選択します。

e) **[サーバー (Server)]** フィールドに、IP アドレスを入力します。

f) **[ユーザー名 (Username)]** と **[パスワード (Password)]** をそれぞれのフィールドに入力します。

g) 「ティック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。

h) **[無視するホスト (Ignore Hosts)]** 領域で、**[無視するホストの追加 (Add Ignore Host)]** をクリックします。

i) **[ホスト名 (Hostname)]** を入力し、「ティック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。

j) **[保存 (Save)]** をクリックして、プロキシ サーバーを設定します。

（注） プロキシ設定が Nexusダッシュボード ファブリック コントローラ アプリケーションに反映されるまで、最大 5 分間待ってください。

ステップ 3 Cisco Nexusダッシュボード ファブリック コントローラ Web UIで、**[フィードバック (Feedback)]** をクリックします。

ステップ 4 **[フィードバック (Feedback)]** パネルで、星をクリックして Nexusダッシュボード ファブリック コントローラ についての感想をお聞かせください。

ステップ 5 **[提案する (Make a suggestion)]** フィールドに、提案/フィードバックを入力します。

ステップ 6 フィードバックについてシスコと連絡を取ることにした場合は、**[シスコからフィードバックについての連絡を受けてもよい (Cisco may contact me about my Feedback)]** チェックボックスをオンにします。

ステップ 7 **[名前 (Name)]** と **[電子メール (Email)]** のフィールドに名前と電子メールを入力します。

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング

リリース 12.1.1e 以降、NDFC と Nexus Dashboard Insights を同じ Nexus Dashboard クラスタで管理モードでホストしてファブリックを管理し、 Nexus Dashboard Insights をホストして同じファブリックをモニタリングできます。NDFC リリース 12.0.2f では、ファブリック ディスカバリ モードの NDFC、つまり、同じ Nexus Dashboard クラスタ上の NDI を使用したモニタモードが

サポートされていることに注意してください。これには、最大 50 のスイッチの最大規模の 4 つの物理的な Nexus Dashboard ノードが必要でした。この機能は、対応するペアの Nexus Dashboard Insights リリース 12.1.1e を備えた NDFC リリースでもサポートされています。

[サービス（Services）]	互換性バージョン
Nexusダッシュボード	2.2.1g
Nexus ダッシュボード Insights	6.1.2
Nexus Dashboard Fabric Controller	12.1.1e

次の表は、Nexus Dashboard のシステム要件を示しています。

仕様	サポートされるスケール
物理的な Nexus Dashboard ノードの数	5
サポートされるスイッチの数	50
Nexus Dashboard Insights でサポートされるフローの数	10000

同じ Nexus Dashboard への NDFC と NDI のインストール

Cisco NDFC は、同じ Nexus Dashboard で Nexus Dashboard Insights と共同主催できます。

はじめる前に

- Cisco Nexus Dashboard の必要なフォーム ファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。
- 『Cisco NDFC インストールおよびアップグレードガイド、リリース 12.1.1e』の「前提条件」セクションに記載されている要件とガイドラインを満たしていることを確認してください。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『Nexus Dashboard ユーザー ガイド』を参照してください。
- DC のアプリケーションセンターへの接続を確立できない場合は、このセクションをスキップして、『Nexus Dashboard ファブリック コントローラ サービスを手動でインストールする』で説明されている手順に従ってください。
- Cisco Nexus Dashboard で、サービスに IP プール アドレスが割り当てられていることを確認します。詳細については、『Cisco Nexus Dashboard ユーザー ガイド』の「クラスタの設定」の項を参照してください。

Nexus Dashboard Insights のインストール

Cisco Nexus Dashboard の必要なフォームファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。

NDFC のインストール

「Cisco Nexus Dashboard ファブリックコントローラのインストール」を参照してください。

Nexus Dashboard で NDFC サイトを設定します。手順については、『Cisco Nexus Dashboard ユーザーガイド』の「サイトの追加」セクションを参照してください。

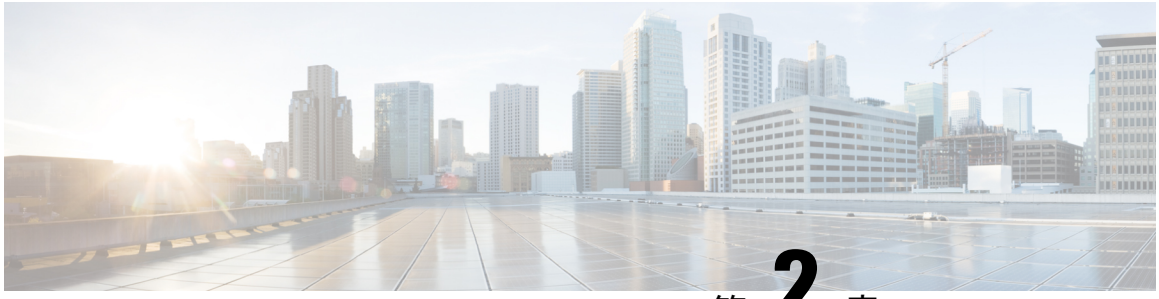
NDI のインストール

同じ Nexus Dashboard セットアップで、Nexus Dashboard Insights サービスをインストールします。詳細については、『Cisco Nexus Dashboard Insights 導入ガイド』を参照してください。

インストール後

NDFC と NDI の互換性のあるバージョンを 5 ノードの物理 Nexus ダッシュボードにインストールした後、NDFC をファブリック（LAN）コントローラとして起動します。ファブリックを作成し、NDFC ファブリックでスイッチを検出してインポートします。Nexus Dashboard は、NDFC ファブリックと [サイト（Sites）] ページのリストをエンティティとして自動的に識別します。

（注） Nexus Dashboard サイトマネージャで、各サイトのパスワードを指定する必要があります。



第 2 章

ダッシュボード

ダッシュボードの目的は、ネットワーク管理者とストレージ管理者がデータセンタースイッチングの健全性とパフォーマンスに関する特定の領域に集中できるようにすることです。この情報は、24 時間のスナップショットとして提供されます。

Cisco SAN コントローラ Web UI で使用できるさまざまなスコープは次のとおりです。

概要

デフォルトでは、使用可能なダッシュレットのサブセットがダッシュボードの概要に自動的に表示されます。

左側のメニューバーから **[ダッシュボード（Dashboard）]** > **[概要（Overview）]**を選択します。**[概要（Overview）]** ウィンドウに次のダッシュレットが表示されます。

[概要（Overview）] ダッシュボードウィンドウに表示されるデフォルトのダッシュレットは次のとおりです。

ダッシュレット	説明
ファブリック	ファブリックの名前、状態、ヘルスステータスなどのファブリックの詳細を表示します。 ファブリックの詳細を表示するには、ファブリック名（リンク）をクリックして **[ファブリック（Fabric）]** スライドインペインを開きます。**[起動（Launch）]** アイコンをクリックします。または、ファブリック名をダブルクリックします。

ダッシュレット	説明
	[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。
イベント分析	**重大**、**メジャー**、**マイナー**、および**警告**の重大度を持つイベントを表示します。 円グラフの重大度レベルまたはセクターをクリックして、イベントおよびアラームの重大度に関する詳細情報を **[イベント分析（Event Analytics）]** ウィンドウに表示します。
Links	データセンターで送受信するための Inter-Switch Link（ISL）および NPV リンクの図を表示します。円グラフのセクターをクリックして、**[SAN リンク（SAN Links）]** ウィンドウに詳細情報を表示します。
スイッチ	**スイッチの状態**：スイッチのヘルスステータスを、括弧内にスイッチの総数とともに色とヘルス状態名を含むグラフの形式で表示します。 色とその意味を次のリストに示します。 • 緑：要素が正常に機能し、意図したとおりに機能していることを示します。 • 黄：要素が警告状態にあり、それ以上の問題を防ぐために注意が必要であることを示します。 • 赤：要素が重大な状態にあり、すぐに対処する必要があることを示します。 • グレー：要素を特定するための情報がないか、要素が検出されたことを示します。 **スイッチステータス**：スイッチのステータスを表示します。 **スイッチリリースバージョン**：スイッチリリースバージョンを表示します。 **スイッチモデル**：スイッチのモデルを表示します。 円グラフのセクター、重大度、ステータス、バージョン、またはモデルをクリックして、

ダッシュレット	説明
	[スイッチ（Switches）] ウィンドウに詳細情報を表示します。
モジュール	モジュールが検出されたスイッチ、モデル名、カウントを表示します。
ポートの使用	ポートインベントリに関する要約情報を表示します。
パフォーマンスコレクタ	パフォーマンスコレクション情報を表示します。 **[更新（Refresh）]** アイコンをクリックしてデータを更新します。 **[コレクタの再始動（Restart collector）]** をクリックして、パフォーマンス収集情報を再始動します。 **[コレクタの停止（Stop collector）]** をクリックして、パフォーマンス収集情報を停止します。
上位の ISL	パフォーマンス上位 10 位 ISL のデータを表示します。各エントリはデバイス名を示し、Rx トラフィックと Tx トラフィックの平均をパーセンテージで指定します。 デバイス名の隣にある **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位の SAN エンドポート	パフォーマンスが高い上位 10 位までの SAN ホストおよびストレージポートのパフォーマンスデータを表示します。各エントリには、現在の受信と送信の割合が表示され、各トランクが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。 デバイス名の隣にある **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位の FICON エンドポート	上位 10 位の FICON ホストおよびコントロールユニットのデータを表示します。各エントリは、スイッチインターフェイスのポートトラフィックを示し、FICON ポートが接続されているデバイスを指定し、Rx トラフィックと Tx トラフィックの平均、および超過したパーセンテージ値を指定します。

ダッシュレット	説明
	デバイス名の隣にある **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位の FCIP ISL	FCIP ISL を実行している上位 10 位のデータを表示します。各エントリはデバイス名を示し、Rx トラフィックと Tx トラフィックの平均、および超過したパーセンテージ値を指定します。 **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位のオプティクス	上位 10 位のオプティクスのデータを表示します。最も高温の SPF、最も低温の SPF、低い受信出力、最も低い送信出力でオプティクスを並べ替えることができます。 スイッチインターフェイスの隣にある **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位の CPU/温度	上位の CPU のデータとスイッチの温度の詳細を表示します。 スイッチの隣にある **[チャート（chart）]** アイコンをクリックして、詳細を表示します。
上位のエラーと破棄	選択したインターフェイスで破棄された上位のエラーパケットを表示します。 **[チャート（chart）]** アイコンをクリックして、詳細を表示します。

ホスト

UI パス：**[ダッシュボード（Dashboard）]** > **[ホスト（Host）]**

ホストダッシュボード：ホストダッシュボードでは、検出されたすべての SAN ホストおよび仮想ホストに関連するすべての情報を確認できます。ホストダッシュボードには、仮想ホストの上位に設定された個々のホストおよび仮想マシンに関する I/O トラフィック、ディスク遅延、CPU、メモリの統計情報、トポロジ、およびイベントなど、ネットワークに関連する非常に詳細な情報が表示されます。**[ホスト（Host）]** ダッシュボードは、次の 4 つのパネルで構成されます。

- **[エンクロージャ（Enclosures）]** パネル：ホストとそのネットワーク属性を一覧表示します。

関連するホスト エンクロージャの **[i]** アイコンをクリックして、SAN Insights モニタリングページを表示します。詳しくは「メトリックのモニタリング」を参照してください。

- **[トラフィックチャート（Traffic Chart）]**：個々のホストまたは仮想マシンに関する I/O 統計情報、CPU とメモリの情報、およびディスク遅延を示します。
- **[イベントテーブル（Event Table）]** タブ：特定のホストエンクロージャ内に設定されたすべてのスイッチポートのイベント情報を示します。
- **[トポロジ（Topology）]** パネル：ホストエンクロージャとストレージエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。検出された仮想マシンが表示され、仮想マシンを選択すると、SANデータソースへのパスが表示されます。このビューを切り替えて、すべてのデータパスを一覧表示できます。
- **[ホスト名（Host Name）]** をクリックすると、スライドインパネルが表示されます。以下のフィールドを表示できます。

次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
[IPアドレス（IP Address）]	スイッチの IP アドレスを表示します。
Mac アドレス	MAC アドレスを表示します。
WWN	ポート WWN を表示します。
FCID	関連する FCID を指定します。
OS	OS の詳細を表示します。
#VMs	VM の数を表示します。
VHost 名	仮想ホストの名前が表示されます。
VHost IP	仮想ホストの IP アドレスの名前を表示します。
VCluster	仮想クラスタの名前を表示します。
マルチパス	マルチパスの詳細を表示します。
プロトコル	ホストが SCSI プロトコルトラフィックまたは NVMe プロトコルトラフィックをストリーミングしているかどうかを指定します。 この列には、SAN Insights を使用して Nexusダッシュボードファブリック コントローラにデータがストリーミングされるホストのデータのみが表示されます。

（注） vCenter設定の収集レベルによって、収集されてグラフに表示されるデータの量が決まります。レベル 1 は、すべての収集間隔のデフォルトの収集レベルです。ディスク I/O 履歴データを収集するには、vCenter 統計設定をレベル 2 以上に変更します。

ホスト ラックの表示

SAN コントローラの Web UI からホストエンクロージャを表示するには、次の手順を実行します。

手順

ステップ 1 **[ダッシュボード（Dashboards）]** > **[ホスト（Hosts）]**を選択します。

ホスト エンクロージャ テーブルのホストのリストが表示されます。

ステップ 2 ホストエンクロージャの **[i]**アイコンをクリックします。

[SAN Insights モニタリング（SAN Insights Monitor）] ウィンドウが表示されます。

ステップ 3 **[SAN Insights モニタリング（SAN Insights Monitor）]** ウィンドウで、必要なホスト名をクリックします。

ホストエンクロージャのスライドインペインが表示されます。

ステップ 4 **[起動（Launch）]**アイコンをクリックして、[ホストエンクロージャ（Host Enclosure）]ページを表示します。

ホスト エンクロージャ ウィンドウが表示されます。

[ホストエンクロージャ] ウィンドウには、選択したホストのイニシエータとターゲット（IT）のペア、トポロジ、平均ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア**：このテーブルには、選択したホストのすべてのイニシエータとターゲットのペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ**：ホストエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの **[表示 （View）]** で、**[+]** または **[-]** をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、**[更新（Refresh）]** をクリックします。**[レイアウトの選択（Select layout）]** ドロップダウンリストを選択して、トポロジを表示します。これは、**階層的（Hierachical）**または**階層的左 - 右（Hierachical Left-Right）**ビューのいずれかです。

- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス**：このテーブルには、選択したインターフェイスに対して選択された過去 1 時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチ インターフェイス テーブルの上部に表示されます。

CPU とメモリおよびディスク I/O チャートの表示

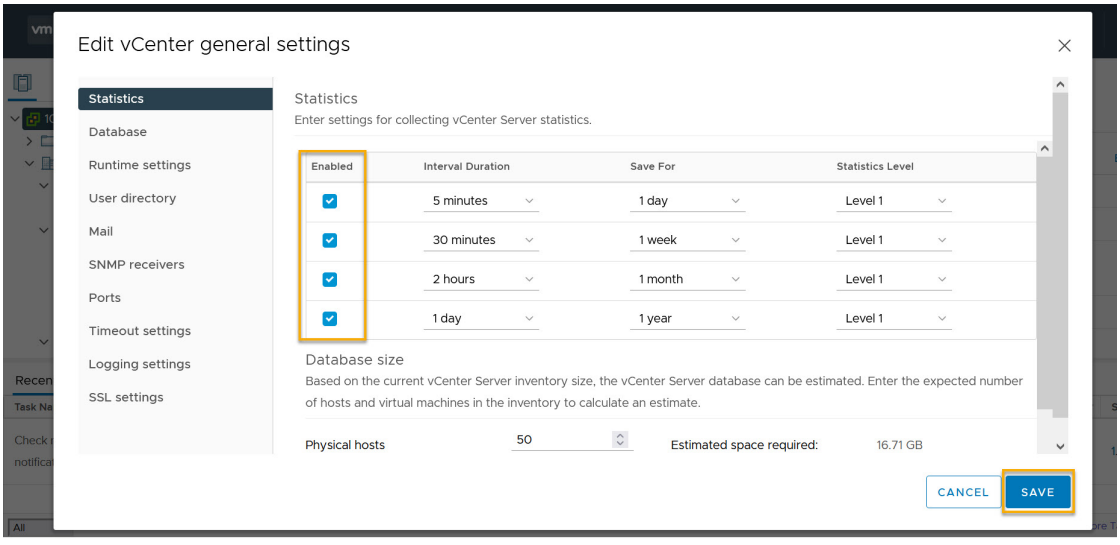
NDFC SAN コントローラ Web UI から SAN ホストエンクロージャを表示するには、次の手順を実行します。

始める前に

[CPU とメモリ（CPU & Memory）] と **[ディスク I/O（Disk I/O）]** の VM チャートを表示するには、vSphere vCenter で vCenter 設定を編集し、統計を手動で有効にする必要があります。

vSphere vCenter で統計情報を手動でイネーブルにするには、次の手順を実行します。

1. vSphere vCenter にログインします。（適切な **[ホスト（Host）]** をクリックします）
2. **[設定（Configure）]**>**[編集（EDIT）]**をクリックします。**[vCenter の一般設定の編集（Edit vCenter general settings）]** 画面が表示されます。
3. **[統計（Statistics）]** タブで、すべてのチェックボックスをオンにして、**[保存（SAVE）]** をクリックします。



手順

ステップ 1 **[ダッシュボード（Dashboards）]** > **[ホスト（Hosts）]**を選択します。

[エンクロージャ（Enclosures ）] テーブルのホストのリストが表示されます。

ステップ 2 ホスト名をクリックします。

[ホスト（Host）] のスライドインペインには、一般的な情報が表示されます。

ステップ 3 **[#VMs]** をクリックして VM を表示します。

[SAN ホスト VM 画面（SAN Host VM Screen）] が表示されます。

エンクロージャを選択して、右側のペインに **[CPU とメモリ（CPU & Memory）]** と **[ディスク I/O（Disk I/O）]** のチャートを表示します。

ストレージ

ストレージダッシュボードにアクセスするには、**[ダッシュボード（Dashboard）]** > **[ストレージ（Storage）]**を選択します。

ストレージダッシュボードは、次の 4 つのパネルで構成されます。

- **[エンクロージャ（Enclosures）]**エリア：ストレージとそのネットワーク属性を一覧表示します。

  関連するホスト エンクロージャの **[i]** アイコンをクリックして、SAN Insights モニタリングページを表示します。詳しくは「メトリックのモニタリング」を参照してください。

- **[トポロジ（Topology）]** エリア — ホストエンクロージャとストレージエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。検出された仮想マシンが表示され、仮想マシンを選択すると、SANデータソースへのパスが表示されます。このビューを切り替えて、すべてのデータパスを一覧表示できます。

- **[トラフィックチャート（Traffic Chart）]** エリア：個々のホストまたは仮想マシンに関する I/O 統計情報、CPU とメモリの情報、およびディスク遅延を示します。

- **[イベントテーブル（Event Table）]**エリア：特定のホストエンクロージャ内に設定されたすべてのスイッチポートのイベント情報を示します。

- **[ストレージ名（Storage Name）]** をクリックすると、スライドインパネルが表示されます。以下のフィールドを表示できます。

次の表では、この画面のフィールドについて説明します。

フィールド	説明
[IPアドレス（IP Address）]	スイッチの IP アドレスを表示します。
Mac アドレス	MAC アドレスを表示します。
WWN	ポート WWN を表示します。
FCID	関連する FCID を指定します。
OS	OS の詳細を表示します。
#VMs	VM の数を表示します。
VHost 名	仮想ホストの名前が表示されます。
VHost IP	仮想ホストの IP アドレスの名前を表示します。
VCluster	仮想クラスタの名前を表示します。
マルチパス	マルチパスの詳細を表示します。
プロトコル	ホストが SCSI プロトコルトラフィックまたは NVMe プロトコルトラフィックをストリーミングしているかどうかを指定します。 この列には、SAN Insights を使用してデータが SAN コントローラにストリーミングされるホストのデータのみが表示されます。

ストレージエンクロージャの表示

SAN コントローラを使用すると、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は**[設定（Settings）]**>**[サーバー設定（Server Settings）]**>**[Insights]**から変更できます。新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

SAN コントローラの Web UI からストレージエンクロージャを表示するには、次の手順を実行します。

手順

ステップ 1 **ダッシュボード（Dashboards）**>**[ストレージ（Storage）]**を選択します。

ストレージ エンクロージャ テーブルのストレージのリストが表示されます。

ステップ 2 **[i]** アイコンをクリックして、SAN Insights モニタリングページを表示します。SAN Insights モニタリングウィンドウで、必要なストレージ名をクリックします。詳しくは「メトリックのモニタリング」を参照してください。

[SAN Insights モニタリング（SAN Insights Monitor）] が表示されます。

ステップ 3 **[起動（Launch）]** アイコンをクリックして、[ストレージエンクロージャ（Storage Enclosure）] ウィンドウを表示します。

ストレージ エンクロージャ ウィンドウが表示されます。

[ストレージエンクロージャ] ウィンドウには、選択したホストのイニシエータとターゲット（IT）のペア、トポロジ、平均 ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア**：このテーブルには、選択したストレージのすべてのイニシエータとターゲットのペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ**：ホストエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの **[表示 （View）]** で、**[+]** または **[-]** をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、**[更新（Refresh）]** をクリックします。**[レイアウトの選択（Select layout）]** ドロップダウンリストを選択して、トポロジを表示します。これは、**階層的（Hierachical）**または**階層的左 - 右（Hierachical Left-Right）**ビューのいずれかです。
- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス**：このテーブルには、選択したインターフェイスに対して選択された過去 1 時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチ インターフェイス テーブルの上部に表示されます。

SAN Insights

SAN Insights は、ファブリックレベルの情報をエンドツーエンドの全体像で視覚的に表示します。

SAN Insights ダッシュボードページで、プロトコル、ファブリック、およびスイッチをプロトコル、ファブリック、およびスイッチのドロップダウンリストから選択できます。ダッシュレットには、選択した範囲に基づいたインサイトデータが表示されます。

ダッシュボードには、過去 72 時間のデータが表示されます。ただし、フローサマリとエンクロージャ サマリ ドーナツには、最新の更新時刻からの最後の 15 分が表示されます。

SAN コントローラを使用すると、ファブリック、スイッチ、および 2 つのプロトコル（SCSI と NVMe）に基づいて SAN Insights メトリックを表示できます。

SAN コントローラの SAN Insights 機能が有効になっていることを確認します。**[設定（Settings）]** > **[機能管理（Feature Management）]**を選択し、**[SAN Insights]** チェックボックスをオンにします。

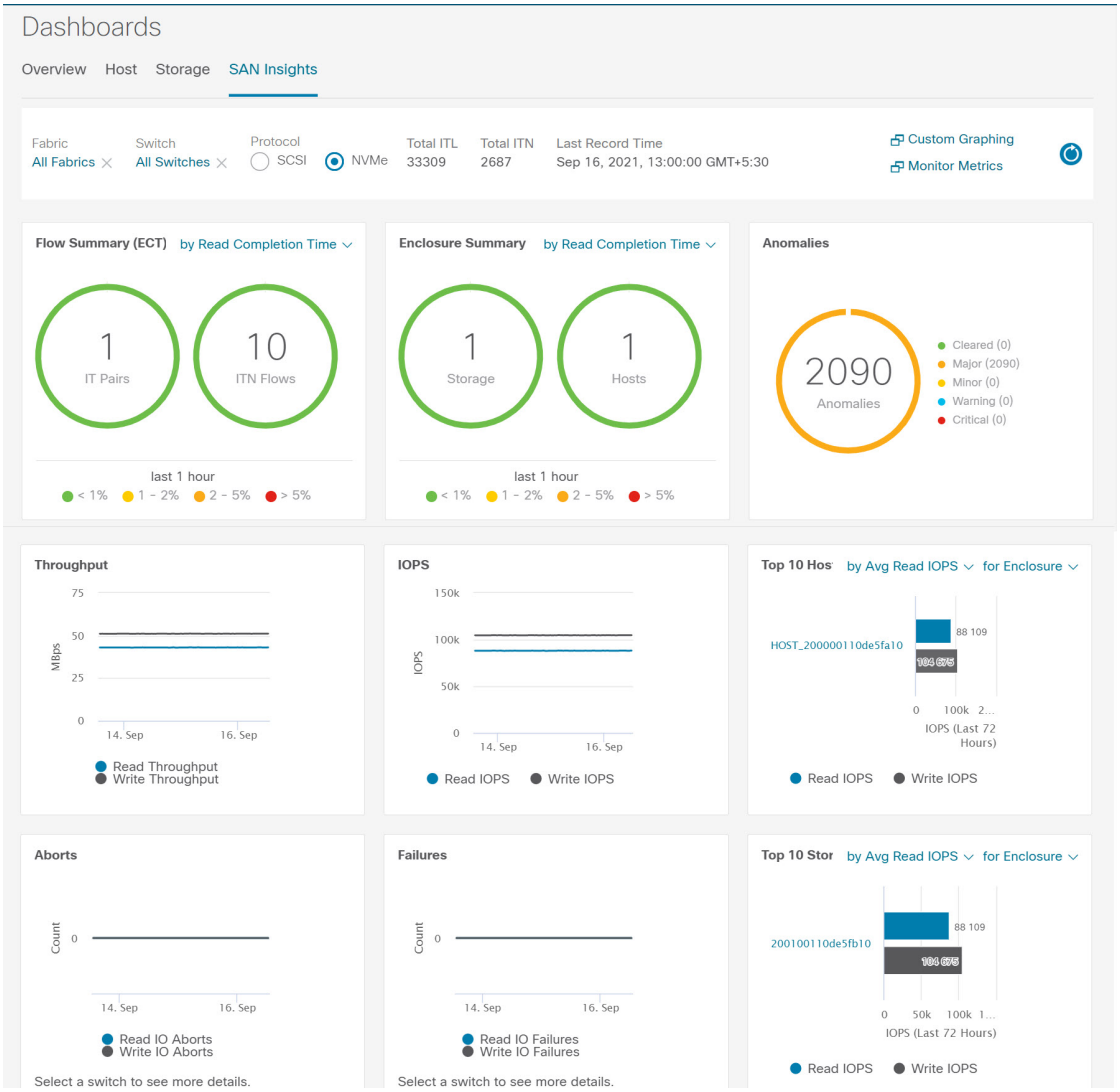
ダッシュボードに情報を表示するために、SAN Insights が構成されていることを確認します。「SAN Insights の設定 （48 ページ）」を参照してください。

SAN Insights の表示

SAN Insights ダッシュボードを表示するには、**[ダッシュボード（Dashboard）]** > **[SAN Insights]** を選択します。SAN Insights ダッシュボードは、全体的な読み取り/書き込み IO 操作/遅延を可視化することができます。

表 *1 : SAN Insights* ダッシュボード

フィールド	説明
ファブリック	**[ファブリック（Fabric）]** をクリックして必要なファブリックを選択し、**[保存（Save）]** をクリックします。
スイッチ	**[スイッチ（Switch）]** をクリックして、必要なスイッチを選択します。
プロトコル	**[SCSI]** または **[NVMe]** チェックボックスを選択して、必要なプロトコルを選択します。 デフォルトでは、**SCSI** プロトコルが選択されます。
合計 ITL	選択したオプションの合計 ITL 値を表示します。
合計 ITN	選択したオプションの合計 ITN 値を表示します。
最終記録時間	選択したオプションの最終記録時間を表示します。
カスタムグラフ	**[カスタムグラフ（Custom Graphing）]** をクリックすると、SAN Insights メトリックの [カスタムグラフ（Custom Graphing）] ウィンドウが表示されます。詳細については、カスタムグラフの表示を参照してください。
メトリクスをモニター	**[メトリックのモニタリング（Monitor Metrics）]** をクリックすると、SAN Insights モニタリングウィンドウが表示されます。詳細については、「メトリックのモニタリング」を参照してください。
リフレッシュ	**[更新（Refresh）]** アイコンをクリックすると、ロード画面が更新されます。



新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

トレーニングされたベースラインからの個別の ITL カウントと ITN カウントの合計は、ダッシュボードの右上隅に表示されます。ドーナツには、過去 15 分間のアクティブな ITL/ITN カウントのみが表示されます。ただし、ITL と ITN の合計数には、選択したスコープのすべての ITL と ITN の数が表示されます。

SAN Insights ダッシュボードには、次のダッシュレットが含まれています。

- フローサマリ（ECT）

  ドロップダウンリストから、[読み取り完了時間] または [書き込み完了時間] を選択します。これに基づいて、ドーナツに IT ペアと ITL フローが表示されます。これらのデータポイントは、Elasticsearch で利用可能な最後の 15 分間のデータに基づいて計算されます。

- エンクロージャの概要（ECT）

ドロップダウンリストから、[読み取り完了時間] または [書き込み完了時間] を選択します。これに基づいて、ドーナツにストレージとホストが表示されます。これらのデータポイントは、Elasticsearch で利用可能な最後の 15 分間のデータに基づいて計算されます。

- 異常

  異常ポリシーの数とその重大度を円グラフとリストで表示します。円グラフには重大度レベルがさまざまなカラーモードで表示され、グラフの横のリストには重大度レベルとそのレベルの異常ポリシーの数が表示されます。

  これらの異常を編集、管理、表示、確認、および消去することができます。**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）]**の順に選択します。

- スループット

  読み取りおよび書き込みのスループットレートを表示します。グラフにマウスを合わせると、そのインスタンスの値が表示されます。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。

- IOPS

  読み取りおよび書き込みIOPのトレンドを表示します。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。

- 中断

  読み取りおよび書き込み中止のトレンドを表示します。これらの折れ線グラフのメトリックは、過去72時間のデータに基づいて計算されます。このメトリックは、Cisco MDS SAN 分析インフラストラクチャによって報告される **read_io_aborts** および **write_io_aborts** メトリックに基づいて計算されます。

  詳細については、スイッチを選択して、ダッシュボードページで選択されているスイッチ IP アドレスの読み取り IO 中止/失敗のカスタムグラフを表示します。

- 障害

  読み取りおよび書き込み失敗のトレンドを表示します。これらの折れ線グラフのメトリックは、過去72時間のデータに基づいて計算されます。このメトリックは、Cisco MDS SAN 分析インフラストラクチャによって報告される **read_io_failures** および **write_io_failures** メトリックに基づいて計算されます。

  詳細については、スイッチを選択して、ダッシュボードページで選択されているスイッチ IP アドレスの読み取り IO 中止/失敗のカスタムグラフを表示します。

- 上位 10 件のホスト

  ドロップダウンリストで選択したメトリックに基づいて、選択したプロトコル/ファブリック/スイッチスコープの上位10件のホストエンクロージャ/WWN/デバイスエイリアスを表します。データは、読み取り/書き込みIOPS、スループット、Exchange 完了時間、データアクセス遅延でソートできます。

- 上位 10 件のストレージ

ドロップダウンリストで選択したメトリックに基づいて、選択したプロトコル/ファブリック/スイッチスコープの上位 10 件のストレージエンクロージャ/WWN/デバイスエイリアスを表します。データは、読み取り/書き込み IOPS、スループット、Exchange 完了時間、データアクセス遅延でソートできます。

（注） 上位 10 件のホストと上位 10 件のストレージは、選択したプロトコル、ファブリック、およびスイッチについて収集された 1 時間ごとのデータに基づいて、過去 72 時間にわたって計算されます。特定の WWPN のエンクロージャ名を変更すると、古いエンクロージャ名の名前は、データが 72 時間後にエージアウトするまで表示されます。

[ダッシュボード（Dashboard）] > [SAN Insights] ウィンドウの上部に、**[高 NPU 負荷が検出されました（HIGH NPU LOAD Detected）]** と警告メッセージが表示されます。この警告は、前の週に 1 つ以上のスイッチに未確認の Syslog イベントがあることを意味します。このイベントは、保存または表示される分析データの可用性に影響を与える可能性があります。警告を削除するには、これらのイベントを確認する必要があります。

[**ダッシュボード（Dashboard）] > [SAN Insights]** ウィンドウの上部に、**[高 ITL 負荷が検出されました（HIGH ITL LOAD Detected）]** と警告メッセージが表示されます。最後の間隔で確認された ITL の数が 20,000 を超えると、警告が表示されます。

NPU および ITL ロードをキャプチャするために、SAN コントローラ デバイス マネージャで Syslog が設定されていることを確認します。**[SAN** > **スイッチ**（SAN Switch）]を選択します。スイッチをクリックすると、スライドパネルが表示されます。**[起動（Launch）]**アイコンをクリックしてスイッチ情報を表示し、**[デバイスマネージャ（Device Manager）]** をクリックします。[デバイスマネージャ（Device Manager）] タブで、**[ログ（Logs）] > [Syslog] > [セットアップ（Setup）]** をクリックします。[作成（Create）] をクリックします。必須パラメータを入力します。[ファシリティ（Facility）] エリアで **[syslog]** オプションボタンを選択していることを確認してください。**[作成（Create）]** をクリックして、SAN コントローラサーバーで Syslog を有効にします。

高 NPU 負荷および高 ITL 負荷を解決するには、**[高 NPU 負荷が検出されました（HIGH NPU LOAD Detected）]** または **[高 ITL 負荷が検出されました（HIGH ITL LOAD Detected）]** リンクをクリックします。**[モニタリング（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** ページが表示されます。イベントのリストは、**タイプ: HIGH_NPU_LOAD** および**タイプ: HIGH_ITL_LOAD** でフィルタ処理されます。すべてのスイッチを選択し、**[確認（Acknowledge）]** をクリックします。これにより、**[高 NPU 負荷が検出されました（HIGH NPU LOAD Detected）]** および **[高 ITL 負荷が検出されました（HIGH ITL LOAD Detected）]** 警告が削除されます。

カスタムグラフの表示

SAN Insights メトリックを表示するには、**[Dashboard]** > **[SAN Insights]**を選択します。[SAN Insights Dashboard] ページが表示されます。**[カスタムグラフの表示（View Custom Graphing）]** をクリックして、SAN Insights メトリックの [カスタムグラフ（Custom Graphing）] ウィンドウを表示します。

ダッシュボードには、過去 72 時間のデータが表示されます。ただし、フローの概要とエンクロージャの概要ドーナツには、最新の更新時刻からの過去1時間の集計が表示されます。上位 10 位のホスト/ストレージ、スループット、IOPS、アボート、障害、グラフはそれぞれのデータを表示します。

Note カスタムグラフページの更新間隔は 5 分です。**[再生（Play）]** アイコンをクリックすると、5 分ごとに自動的に更新されます。

Cisco SAN Controller を使用すると、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は、**[Web UI]** > **[設定（Settings）]** > **[サーバー設定（Server Settings）]** > **[Insights]**から変更できます。

新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

カスタムグラフとテーブルの表示

これはフリースタイルダッシュボードで、複数のメトリックを選択でき、選択したメトリックのリアルタイムデータが5分ごとに更新されるように構成された複数線グラフで表示され、対応する生データがデータテーブルに表示されます。

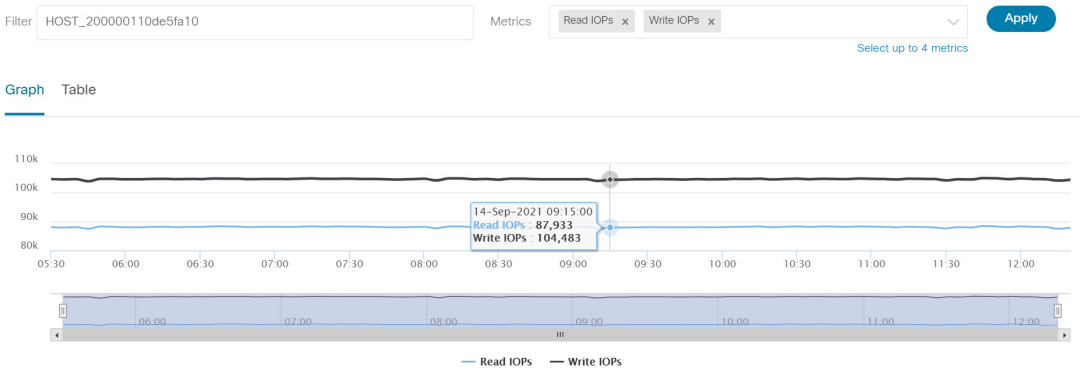
右上の**[グラフの追加（Add Graph）]**をクリックして、比較のために複数のグラフを追加することもできます。

（注） 自動更新オプションはデフォルトで無効になっています。自動更新機能を有効にするには、**[再生（Play）]** アイコンをクリックする必要があります。

SAN Insights メトリックには 2 つのタブがあります。

- グラフ
- 表

グラフ



グラフは、開始日と終了日が選択された対応するメトリックとともにプロットされます。データは5分ごとに更新でき、一時停止ボタンを使用して静的グラフに変換できるため、本質的に動的です。**[グラフの追加（Add Graph）]** をクリックします。このページでは、一度に最大 3 つのグラフを追加できます。

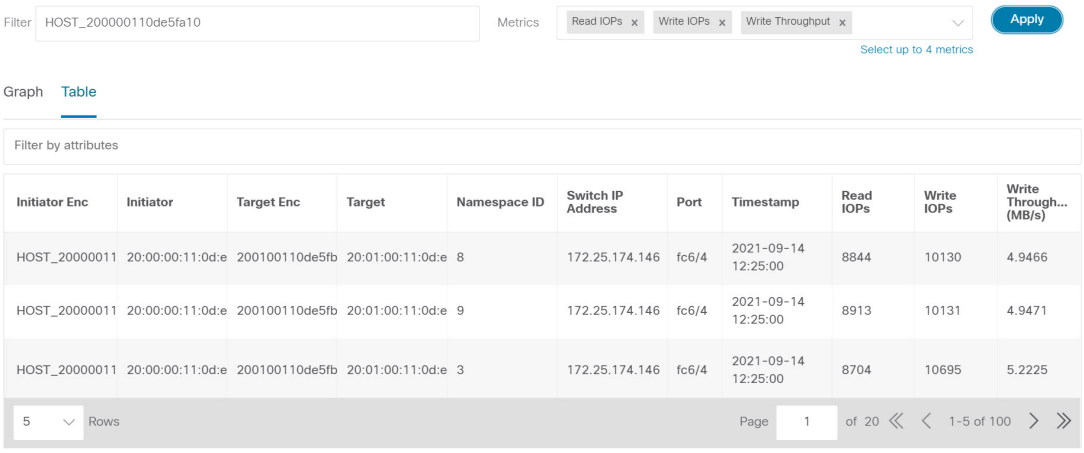
SAN コントローラを使用すると、ユーザーは 2 週間以上（デフォルトの最大 90 日まで）データを表示できます。この時間枠は、サーバーのプロパティで設定できます。[時間範囲（Time Range）] の横にあるドロップダウンボタンをクリックし、日付を選択します。

カスタムグラフのメトリックが拡張され、ドロップダウン メトリック リストに書き込み IO エラー、読み取り IO エラー、書き込み IO の中断、読み取り IO の中断が含まれるようになりました。

各 ITL フロー（読み取りおよび書き込み）の ECT ベースラインは、トレーニング期間にわたって継続的に学習された加重平均を使用して計算されます。

- ECT ベースラインの計算は、トレーニング期間と再調整時間の 2 つの部分で構成されます。
- ECT ベースラインのトレーニング期間は、デフォルトで 7 日間です（設定可能）。
- トレーニングの完了後、ECT ベースラインは、デフォルトで 7 日後に再キャリブレーションがトリガーされるまで同じままです（設定可能）。
- デフォルトでは、14 日ごとにトレーニングが 7 日間（周期的に）実行されます。
- パーセント（%）偏差は、ECT ベースラインと比較した現在の正規化された ECT の偏差を示します。

テーブル



[メトリック（Metrics）]ドロップダウンリストから失敗または中止を選択すると、テーブルリストがフィルタ処理され、選択した失敗または中止のメトリックの少なくとも1つをゼロ以外のエントリとして持つ行のみが表示されます。テーブルには100レコードのみが表示されます。ただし、ゼロ以外のエラーを見つけやすくするために、テーブルをフィルタ処理して、ゼロ以外の中止または失敗を持つ最後の100レコードを表示することができます。失敗または中止を選択すると、テーブルラベルがこの動作を表すように変更されます。

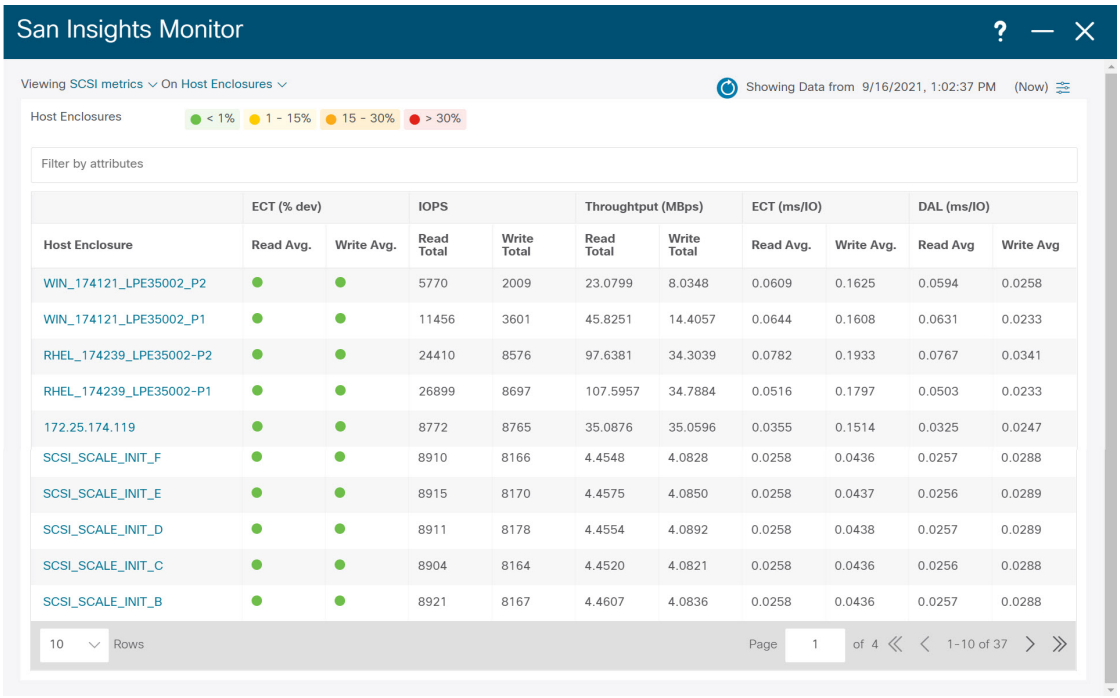
表示するには、属性別フィルタ処理フィールドに7つのディメンション（イニシエータEnc、イニシエータ、ターゲットEnc、ターゲット、LUN、スイッチIPアドレス、ポート、タイムスタンプ、読み取りIOP、書き込みIOP）のいずれかを入力し（コンマで区切って）、関連するメトリックを選択します。

メトリックのモニタリング

UIパス：**[ダッシュボード（Dashboard）]** > **[SAN Insights]** > **[メトリックのモニタリング（Monitor Metrics）]**

[SAN Insights モニタ（SAN Insights Monitor）] ページには、環境内の問題をすばやく特定できるように、インターフェイスにヘルス関連のインジケータが表示されます。ヘルスインジケータを使用して、ファブリックのどこに問題があるかを理解できます。

SANコントローラを使用すると、SCSIとNVMeの2つのプロトコルに基づいてSAN Insightsモニタを表示できます。デフォルトでは、SCSIプロトコルが選択されます。ただし、この設定は**[設定（Settings）]** > **[サーバー設定（Server Settings）]** > **[Insights]**から変更できます。



リリース 12.0.1a から、ダッシュボードに SAN Insights モニタリングを表示できます。SAN コントローラ Web UI から、次の手順を実行します。

手順

ステップ 1 **[Dashboard]** > **[SAN Insights]** を選択します。

ステップ 2 **[メトリックのモニタリング（Monitor Metrics）]** をクリックします。

[SAN Insights モニタリング（SAN Insights Monitor）] ウィンドウが表示されます。

ステータスの色は、それぞれのイニシエータターゲットペアの読み取り偏差と書き込み偏差の時間平均です。

ステップ 3 **[表示（Viewing）]** ドロップダウンリストを使用して **SCSI** または **NVMe** メトリックを選択して表示し、データタイプを選択します。

ステップ 4 **[オン（On）]** ドロップダウンリストを使用して、**[ホストエンクロージャ（Host Enclosure）]**、**[ストレージエンクロージャ（Storage Enclosure）]**、または **[IT ペア（IT Pairs）]** を選択して、必要なデータを表示します。

ステップ 5 **[更新（Refresh）]** アイコンをクリックして、現在の時刻を表示します。

ウィンドウの右隅にシステム時刻が表示されます。

時間設定アイコンを使用して時間間隔を指定します。**[設定（Setting）]** アイコンをクリックし、適切な時間を時間単位で入力し、**[適用（Apply）]** をクリックして、選択した時間のデータを表示します。

トポロジページのスイッチで緑色の円のアイコンを選択すると、スイッチ インターフェイス カウンタが表示されます。

ステップ 6 必要な名前をクリックして詳細を表示します。

関連する IT ペアがスライドインパネルに表示されます。

ステップ 7 **[起動（Launch）]** アイコンをクリックして、ウィンドウを表示します。

同様に、名前を 3 回クリックすると、詳細ビューに移動できます。

[SAN Insights モニタ（SAN Insights Monitor）] ページには、選択したエンクロージャまたは IT ペアのイニシエータとターゲットのペアが表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、ECT（%dev）、IOPS、スループット情報に関するすべてのメトリックの詳細が表示されます。

同様に、ダッシュボードのホストおよびストレージタブから SAN Insights モニタを表示できます。

- **[ダッシュボード（Dashboard）] > [ホスト（Host）]** を選択し、必要なホスト名の **[i]** アイコンをクリックします。ホストエンクロージャの詳細については、ホストセクションを参照してください。
- **[ダッシュボード（Dashboard）] > [ストレージ（Storage）]** を選択し、必要なストレージ名の **[i]** アイコンをクリックします。ストレージエンクロージャの詳細については、ストレージセクションを参照してください。

イニシエータとターゲット（IT）のペアの詳細については、「IT ペアの表示 （25 ページ）」セクションを参照してください。

IT ペアの表示

Cisco Nexusダッシュボード ファブリック コントローラ では、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は**[設定（Settings）] > [サーバー設定（Server Settings）] > [Insights]**から変更できます。新しいプロパティを使用するには、SAN Insights サービスを再起動してください

Cisco Nexusダッシュボード ファブリック コントローラ Web UI から IT ペアを表示するには、次の手順を実行します。

始める前に

UI パス：**[ダッシュボード（Dashboard）] > [SAN Insights] > [メトリックのモニタリング（Monitor Metrics）]**

手順

ステップ 1 **[ダッシュボード（Dashboard）]** > **[SAN Insights]** > **[メトリックのモニタリング（Monitor Metrics）]**を選択します

SAN Insights モニタリングページが表示されます。詳しくは「メトリックのモニタリング」を参照してください。

ステップ 2 **[表示（Viewing）]** ドロップダウンリストを使用して **SCSI** または **NVMe** メトリックを選択して表示し、データタイプを選択します。

ステップ 3 データを表示するには、**[オン（On）]** ドロップダウンリストを使用して **[IT ペア（IT Pairs）]** を選択します。

ステップ 4 必要な IT ペア名をクリックします。

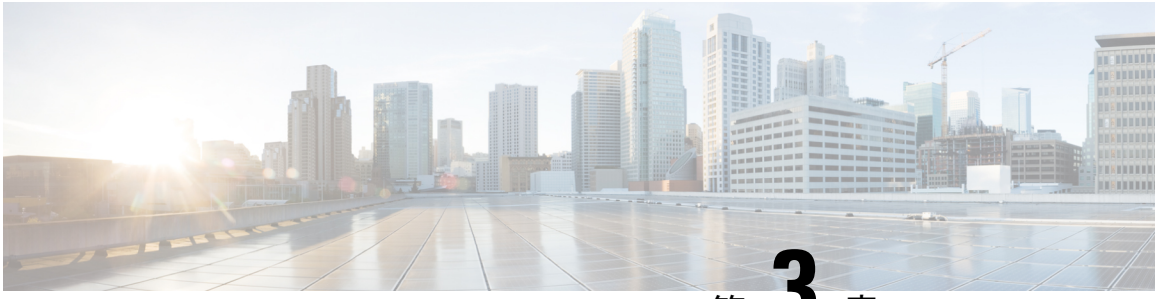
IT ペアのスライドインパネルが表示されます。

ステップ 5 **[起動（Launch）]** アイコンをクリックして、IT ペアウィンドウを表示します。

IT ペアのウィンドウが表示されます。

IT ペアウィンドウには、選択した IT ペアのイニシエータとターゲット (IT) ペア、トポロジ、平均 ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア** - このテーブルには、選択した IT ペア名のすべての IT ペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ**： IT ペア間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの **[表示 （View）]** で、**[+]** または **[-]** をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、**[更新（Refresh）]** をクリックします。**[レイアウトの選択（Select layout）]** ドロップダウンリストを選択して、トポロジを表示します。これは、**階層的（Hierachical）**または**階層的左 - 右（Hierachical Left-Right）**ビューのいずれかです。
- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス**：このテーブルには、選択したインターフェイスに対して選択された過去 1 時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチ インターフェイス テーブルの上部に表示されます。



第 3 章

トポロジ

UI ナビゲーション : [トポロジ（Topology）] をクリックします。

[トポロジ（Topology）] ウィンドウには、スイッチ、リンク、ファブリックエクステンダ、ポート チャネル設定、仮想ポート チャネルなど、さまざまなネットワーク要素に対応する色分けされたノードとリンクが表示されます。このウィンドウを使用して、次のタスクを実行します。

- これらの各要素の詳細を表示するには、対応する要素の上にカーソルを移動します。
- トポロジのナビゲーションを表示するには、上部のパンくずリストを表示します。
- デバイスまたは要素をクリックすると、右側にスライドインペインが表示され、デバイスまたは要素に関する詳細情報が表示されます。トポロジの詳細を表示するには、ノードをダブルクリックしてノード トポロジを開きます。たとえば、**[トポロジ（Topology）]** ウィンドウでファブリック トポロジとそのコンポーネントを表示するには、ファブリック ノードをダブルクリックしてから、表示する要素（ホスト、マルチキャスト グループ、マルチキャスト フローなど）をダブルクリックし、ファブリック タイプを表示します。
- ファブリックのファブリック サマリを表示する場合は、ファブリック ノードをクリックします。**[ファブリック サマリ（Fabric Summary）]** スライドイン ペインから、**[ファブリックの概要（Fabric Overview）]** ウィンドウを開きます。または、ファブリックを右クリックして **[詳細表示（Detailed View）]** を選択し、**[ファブリックの概要（Fabric Overview）]** ウィンドウを開きます。[ファブリックの概要（Fabric Overview）]ウィンドウの詳細については、ファブリックの概要 （56 ページ） を参照してください。
- 同様に、スイッチをクリックすると、設定されたスイッチ名、IP アドレス、スイッチ モデル、およびステータス、シリアル番号、正常性、最後にポーリングされた CPU 使用率、最後にポーリングされたメモリ使用率などのその他のサマリー情報が **[スイッチ（Switch）]** スライドインペインに表示されます。 -inペイン。詳細を表示するには、**[起動（Launch）]** アイコンをクリックして、**[スイッチの概要（Switch Overview）]** ウィンドウを開きます。[スイッチの概要（Switch Overview）] ウィンドウの詳細については、スイッチの概要 （78 ページ） を参照してください。

  SAN スイッチの役割は、コア ルータとエッジ ルータの2つだけです。

- **[アクション（Actions）]** ドロップダウン リストからアクションを選択し、トポロジで選択した要素に基づいてさまざまなアクションを実行します。
- トポロジ内の要素に対してアクションを実行するには、アクション ドロップダウン リストにリストされている要素以外の要素を右クリックします。これにより、適切なウィンドウが開き、要素に基づいてタスクを実行できます。たとえば、ファブリックを右クリックすると、さまざまな設定、ファブリックの削除、バックアップと復元などのタスクを実行できます。

この項の内容は、次のとおりです。

トポロジの検索

効果的な検索を行うには、検索バーで検索属性と検索条件の組み合わせを使用します。検索属性と検索条件の組み合わせを検索バーに入力すると、対応するデバイスがトポロジ内で強調表示されます。

等号（=）、不等号（!=）、次を含む（**contains**）、次を含まない（**!contains**）などの検索条件を適用できます。

SAN ファブリックに使用できる検索属性はファブリック名です。

トポロジにデバイスが表示されたら、そのデバイスをダブルクリックしてトポロジ内をさらに移動します。たとえば、検索したファブリックがトポロジに表示されている場合は、ファブリック（クラウド アイコン）をダブル クリックしてトポロジ内を移動します。さらに、ファブリックがトポロジに表示された後、条件とスイッチ名、IPアドレス、モデル、シリアル、ソフトウェアバージョン、およびアップタイムなどの条件とさまざまな検索持続性に基づいて検索を続行できます。

（注） トポロジの特定のレベルではフィルタのみが許可されます。つまり、フィルタは検索の代わりに使用されます。これらのレベルのトポロジリストには、限られた数のエンティティが表示されます。

トポロジの表示

移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

スイッチを複数選択する場合、マウスドラッグを放してスイッチの選択を終了する前に、修飾キー（cmd/ctrl）を放す必要があります。

[表示（View）] ペインでは、デバイスとリンクに関する次の情報を表示できます。

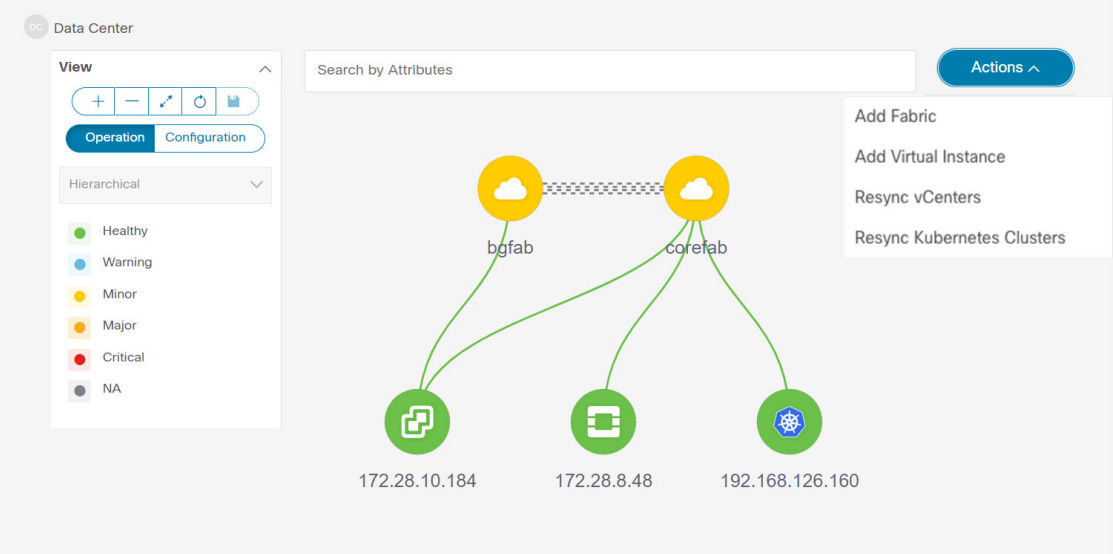
- レイアウトオプション：画面に合わせてレイアウトを拡大、縮小、または調整できます。トポロジを更新したり、トポロジへの変更を保存したりすることもできます。詳細については、ズーム、パン、ドラッグ （31 ページ）を参照してください。
- [レイアウトの選択（Select Layout）]ドロップダウン リスト：このドロップダウン リストからトポロジのレイアウトを選択し、レイアウトオプションで**[トポロジ レイアウトの保存（Save Topology Layout）]** をクリックします。詳細については、レイアウト （32 ページ）を参照してください。
- ステータス：すべてのデバイスまたはリンクのステータスが異なる色で表示されます。LAN トポロジの構成ステータスと動作ステータスも表示できます。詳細については、ステータス （32 ページ）を参照してください。

ノードのトポロジは、複数のスコープで表示されます。各スコープは、階層順に表示されます。スコープ階層はトピックパス（パンくずリスト）として表示され、必要なスコープに移動できます。スコープは次のとおりです。

- Data Center
- クラスタ（VCenter）
- リソースリスト（DVS、コンピューティング、および VM）
- Resource

（注）

- **[トポロジ（Topology）]** ウィンドウでは、FEX の操作と構成ステータスが計算されないため、FEXはグレー（**[未知（Unknown）]** または **[該当なし（NA）]**）で表示されます。
- あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは **[トポロジ（Topology）]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。



SAN トポロジの要素の表示

UI ナビゲーション：[トポロジ（Topology）] をクリックします。

ここでは、SAN ファブリックの **[トポロジ（Topology）]** ウィンドウに表示されるさまざまな要素またはエンティティについて説明します。

VSAN

[トポロジ（Topology）] ウィンドウで、ファブリックをダブルクリックしてファブリック トポロジを表示します。SAN ファブリックには、VSAN ノードとスイッチが含まれます。VSAN ノードには、カッコ内に数字が表示され、ファブリック内の VSAN の数を示します。VSAN ノード トポロジ内の個々の VSAN を表示するには、VSAN ノードをダブルクリックします。

VSAN トポロジには、VSAN に接続されているゾーンとスイッチが表示されます。VSAN をダブルクリックして VSAN トポロジを開き、ゾーンとスイッチを表示します。ただし、スイッチには VSAN が設定され、VSAN メンバーシップを持つリンクが必要です。

ゾーン

VSAN ノードをダブルクリックすると、VSAN ゾーンが表示されます。その VSAN およびゾーン ノードのスイッチは、ゾーンの数を示します。そのゾーン ノードをダブルクリックすると、個々のゾーン ノードが表示されます。ゾーン ノードをダブルクリックすると、そのゾーンのスイッチと、選択したゾーンのメンバーであるエンド デバイスとの接続（ISL）が表示されます。

ホストとストレージ

ゾーン トポロジには、ゾーンに関連し、スイッチに接続されているホストとストレージ デバイスが表示されます。**[トポロジ（Topology）]** ウィンドウで、ゾーンをダブルクリックしてホストとストレージ デバイスを表示します。

または、スイッチ トポロジを表示するには、ファブリック トポロジ内のスイッチを直接クリックします。スイッチ トポロジには、スイッチに接続されているホストとストレージ デバイスが表示されます。

ホスト

ホスト デバイスをクリックすると、スライドイン ペインにホストに関する詳細情報が表示されます。スライドイン ペインから、ホスト ダッシュボードを開くことができます。または、ホストデバイスを右クリックし、**[詳細表示（Detailed View）]** をクリックしてホスト ダッシュボードを開くこともできます。

ストレージ

ストレージ デバイスをクリックすると、ストレージの詳細情報がスライドイン ペインに表示されます。スライドイン ペインから、ストレージ ダッシュボードを開くことができます。または、ストレージ デバイスを右クリックして **[詳細ビュー（Detailed View）]** をクリックし、ストレージ ダッシュボードを開きます。

Links

スイッチ トポロジで、2 つのデバイス（スイッチとストレージなど）を接続するリンクをクリックして、**[リンク（Link）]** スライドイン ペインを開きます。このペインには、パフォーマンス データの最後のポーリングに関する詳細が表示されます。ただし、**[パフォーマンス データ収集設定（Performance Data Collection Settings）]** でファブリックのパフォーマンス モニタリングを設定しておく必要があります。これにより、Nexusダッシュボードファブリック コントローラはトラフィック情報を収集でき、集約された情報がトラフィック使用率を示すグラフとともに表示されます。Nexusダッシュボード ファブリック コントローラ は、ファブリック内のすべてのスイッチのすべてのポート、リンクなどについて、5 分ごとに最後のポーリング メトリックを更新します。このペインに表示される日時が最新の場合、最後のポーリング メトリックの詳細は最新です。このスライドイン ペインに表示される詳細は次のとおりです。

- リンク キャパシティ、VSAN、ステータスなどの一般情報。
- 平均、最大、および最小の Rx および Tx などの詳細を含む、過去 24 時間のトラフィックに関する情報（バイト単位）。
- Time、Rx、Tx などの最後のポーリング メトリックは、**[グラフ（Graph）]** タブのグラフと **[テーブル（Table）]** タブのテーブル形式で表示できます。テーブルがページ分割されていることに注意してください。

ズーム、パン、ドラッグ

ズームインまたはズームアウトするには、ウィンドウの左下にあるコントロールを使用するか、マウスのホイールを使用します。

移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。

スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

レイアウト

トポロジは、トポロジの配置方法を記憶する **[レイアウトの保存（Save Layout）]** オプションとともに、さまざまなレイアウトをサポートします。

- **[Hierarchical]** および **[Hierarchical Left-Right]**：トポロジのアーキテクチャ ビューを提供します。CLOS トポロジの設定方法に関するノードを示すさまざまなスイッチ ロールを定義できます。

Note 大規模なセットアップを実行する場合、リーフ層のすべてのスイッチを簡単に表示できるようになるのは困難です。これを軽減するために、Nexusダッシュボード ファブリック コントローラは 16 のスイッチごとにリーフ層を分割します。

- **Circular** および **Tiered-Circular**：ノードを円形または同心円状に描画します。
- **[ランダム（Random）]**：ノードはウィンドウにランダムに配置されます。Nexusダッシュボード ファブリック コントローラ は、推測を行い、近接するノードをインテリジェントに配置しようとします。
- **カスタム保存レイアウト**：ノードは、必要に応じてドラッグできます。必要に応じて配置した後、**[保存（Save）]** をクリックして位置を保持します。次回トポロジにアクセスすると、Nexusダッシュボード ファブリック コントローラ により最後に保存したレイアウト位置に基づいてノードが描画されます。

レイアウトを選択する前に、Nexusダッシュボード ファブリック コントローラ はカスタム レイアウトが適用されているかどうかを確認します。カスタム レイアウトが適用されている場合は、それを使用します。Nexusダッシュボード ファブリック コントローラカスタム レイアウトが適用されていない場合は、Nexusダッシュボード ファブリック コントローラ はスイッチが異なる階層に存在するかどうかを確認し、階層レイアウトまたは階層左右レイアウトを選択します。他のすべてのレイアウトが失敗した場合は、強制指向レイアウトが選択されます。

ステータス

各ノードとリンクの色分けは、その状態に対応しています。動作の色とその意味を次のリストに示します。

- 緑：要素が正常に機能し、意図したとおりに機能していることを示します。
- 青：要素が警告状態にあり、それ以上の問題を防ぐために注意が必要であることを示します。
- 黄色：要素に小さな問題があることを示します。
- オレンジ：要素に重大な問題があり、それ以上の問題を回避するには注意が必要であることを示します。

- 赤：要素が重大な状態にあり、すぐに対処する必要があることを示します。
- グレー：要素を特定するための情報がないか、要素が検出されたことを示します。

設定の色とその意味を次のリストに示します。

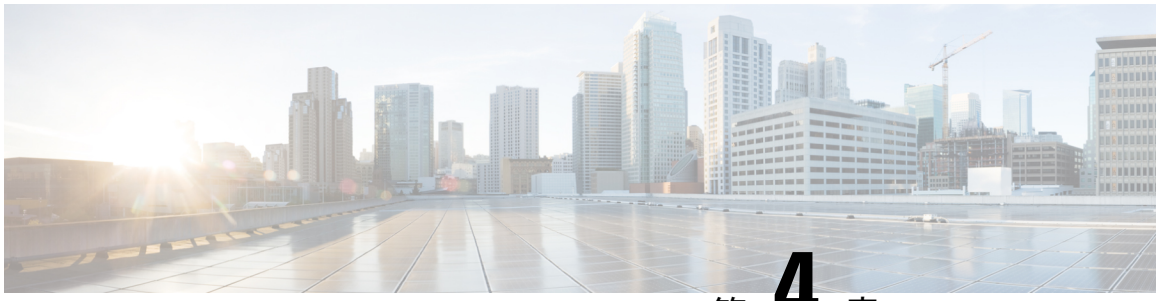
- 緑：要素が目的の設定と同期していることを示します。
- 青：要素に保留中の展開があることを示します。
- 黄色：アクティブな展開が進行中であることを示します。
- 赤：要素が意図した構成と同期していないことを示します。
- グレー：情報が不足しているか、設定の同期計算がサポートされていないことを示します。

Note

- **[トポロジ（Topology）]** ウィンドウでは、FEX の操作と構成ステータスが計算されないため、FEXはグレー（**[不明（Unknown）]** または **[n/a]**）で表示されます。
- あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは **[トポロジ（Topology）]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。

第 I 部

SAN



第 4 章

ファブリック

ファブリック

リリース 12.0.1a から、SAN コントローラを使用して SAN ファブリックを作成できるようになりました。

次の表では、**[SAN コントローラ（SAN Controller）] > [SAN] > [ファブリック（Fabirics）] > [ファブリック（Fabrics）]** で表示されるフィールドについて説明します。

フィールド	説明
Fabric Name（ファブリック名）	ファブリックの名前を指定します。
シード スイッチ	ファブリック内のスイッチを検出するために使用されるシードスイッチを指定します。
状態	ファブリックの状態を指定します。
SNMPv3 / SSH	SNMP および SSH アクセスを許可するかどうかを指定します。
ユーザー/コミュニティ	ファブリックを作成したユーザーのロールを指定します。
認証/プライバシー	認証タイプを表示します。
ライセンス有効	ファブリック内のすべてのスイッチにライセンスがあるかどうかを指定します。
ヘルス（Health）	ファブリックのヘルスを表示します。
パフォーマンス収集	ファブリックでパフォーマンス収集を有効にするか無効にするかを指定します。
更新時刻	ファブリックが作成または更新された時刻を指定します。

フィールド	説明
含める VSANS	ファブリックに含まれる VSANS を指定します。
除外する VSANS	除外する VSANS を指定します。

次の表で、**[SAN] > [ファブリック（Fabrics）] > [ファブリック（Fabrics）]** で表示される [アクション（Actions）] メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
ファブリックの追加	**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの追加（Add Fabric）]** を選択します。手順については、ファブリックの追加 （39 ページ）を参照してください。
ファブリックの編集	編集するファブリックを選択します。**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの編集（Edit Fabrics）]** を選択します。必要な変更を行って、[適用（Apply）] をクリックします。手順については、ファブリックの編集 （40 ページ）を参照してください。
ファブリックの削除	削除する 1 つ以上のファブリックを選択します。**[アクション (Actions)]** ドロップダウンリストで、**[ファブリックの削除 (Delete Fabrics)]** を選択します。**[確認（Confirm）]** をクリックして、ファブリックを削除します。手順については、ファブリックを削除しています（40 ページ）を参照してください。
ファブリックの再検出	ファブリックに関連付けられたスイッチ、リンク、およびエンドデバイスを再検出できます。再検出する 1 つ以上のファブリックを選択します。**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの再検出（Rediscover Fabrics）]** を選択します。**[状態（State）]** 列の進捗バーに、再検出の進行状況が表示されます。手順については、ファブリックの再検出 （41 ページ）を参照してください。
ファブリックの消去	ファブリックの存在しないスイッチ、リンク、およびエンドデバイスを消去できます。消去する 1 つ以上のファブリックを選択します。**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの消去（Purge Fabrics）]** を選択します。手順については、ファブリックの消去 （41 ページ）を参照してください。

アクション項目	説明
パフォーマンスの設定	ファブリックに関連付けられたリンク、スイッチ インターフェイス、およびエンドデバイスのパフォーマンス モニタリングを有効にすることができます。パフォーマンスモニタリング用に 1 つ以上のファブリックを選択します。**[アクション（Actions）]** ドロップダウンリストで、**[パフォーマンスの設定（Configure Performance）]** を選択します。必要な変更を行って、[適用（Apply）] をクリックします。 詳細な手順については、パフォーマンスの設定を参照してください。
SAN Insights の設定	選択したファブリックで SAN Insights を設定できます。 詳細については、SAN Insights の設定を参照してください。
バックアップの設定	ファブリックデータのバックアップを設定およびスケジュールできます。 手順については、ファブリック バックアップの構成（54 ページ）を参照してください。

この章は、次の項で構成されています。

ファブリックの追加

Cisco SAN コントローラ Web UI を使用してファブリックを作成するには、次の手順を実行します。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）] > [SAN ファブリック（SAN Fabrics）]** を選択します。

ステップ 2 **[アクション（Actions）] > [ファブリックの追加（Add Fabrics）]**を選択します。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドに一意のファブリック名を入力します。

ステップ 4 [ファブリックシードスイッチ（Fabric Seed Switch）] テキストボックスにシードスイッチの IP アドレスを入力します。

シードスイッチの DNS 名を入力することもできます。

ステップ 5 アクセスを有効にするには、SNMPv3/SSH チェックボックスをオンにします。

ステップ 6 **[認証/プライバシー（Authentication/Privacy）]** ドロップダウンリストから、スイッチの検出に適切な認証を選択します。

ステップ 7 シードスイッチにアクセスするためのユーザー名とパスワードを適切なフィールドに入力します。

ステップ 8 VSAN のみを使用してスイッチを検出するには、[VSAN による検出の制限（Limit Discovery by VSAN）] チェックボックスをオンにします。

VSAN に関連付けられているスイッチまたは関連付けられていないスイッチを検出することを選択できます。

ステップ 9 （任意） UCS ログイン情報を使用してスイッチを検出することもできます。

ステップ 10 **[追加（Add）]** をクリックして、ファブリックを追加します。

ファブリックの編集

Cisco SAN コントローラ Web UI ファブリックを編集するには、次の手順を実行します。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）] > [SAN ファブリック（SAN Fabrics）]** を選択します。

ステップ 2 チェックボックスをオンにして、必要なファブリック名を編集し、**[アクション（Actions）] > [ファブリックの編集（Edit Fabrics）]** を選択します。

ステップ 3 **[ファブリックの編集（Edit Fabrics）]** ウィンドウが表示されます。一度に編集できるファブリックは 1 つだけです。

ステップ 4 新しいファブリックの **[ファブリック名（Fabric Name）]** を入力します。

ステップ 5 （任意） **[SNMPV3]** チェックボックスをオンにします。SNMPV3 をオンにすると、**[コミュニティ（Community）]** フィールドが **[ユーザー名（User Name）]** および **[パスワード（Password）]** に変わります。

ステップ 6 **[ユーザー名（Username）]** と **[パスワード（Password）]**、プライバシーを入力し、いずれかのステータスオプションを選択することで、SAN コントローラ Web クライアントでファブリックを管理する方法を指定します。

ステップ 7 ステータスを **[管理（Managed）]**、**[非管理（Unmanaged）]**、または **[継続的に管理（Managed Continuously）]** に変更します。

ステップ 8 （任意） **[UCS ログイン情報を使用（Use UCS Credentials）]** チェックボックスをオンにします。UCS ログイン情報を変更する場合。

ステップ 9 **[ユーザー名（Username）]** と **[パスワード（Password）]** を入力します。

ステップ 10 [適用（Apply）] をクリックし、変更を保存します。

ファブリックを削除しています

SAN コントローラ Web UI を使用してファブリックを削除するには、次の手順を実行します。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）] > [SAN ファブリック（SAN Fabrics）]** を選択します。

ステップ 2 **[アクション（Actions）] > [ファブリックの削除（Delete Fabrics）]**を選択して、データソースからファブリックを削除し、そのファブリックのデータ収集を中止します。

ファブリックの再検出

Cisco SAN コントローラ Web UI を使用してファブリックを削除するには、次の手順を実行します。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）] > [SAN ファブリック（SAN Fabrics）]** を選択します。

ステップ 2 チェックボックスを選択して必要なファブリック名を再検出し、**[アクション（Actions）] > [ファブリックの再検出（Rediscover Fabrics）]**を選択します。

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

ファブリックウィンドウの **[状態（State）]** 列には、選択したファブリックの再検出の進行状況が表示されます。

ファブリックが再検出されました。

ファブリックの消去

[消去（パージ）]オプションを使用して、ファブリック 検出テーブルをクリーニングおよび更新できます。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）]** を選択します。

ステップ 2 消去するファブリックの横にあるチェックボックスをオンにします。

ステップ 3 **[アクション（Actions）] > [ファブリックの消去（Purge Fabrics）]** を選択します。

ファブリックは消去されます。

SANコントローラリリース12.0.1aから、トポロジウィンドウでファブリックを消去できます。

- **[トポロジ（Topology）]** を選択し、ファブリックを選択し、ファブリックを右クリックして、**[ファブリックを消去する（Purge Down Fabric）]** を選択します。

ファブリックは消去されます。

パフォーマンスの設定

パフォーマンスマネージャを使用してファブリックを管理する場合は、ファブリック上でフローおよび収集の初期セットを設定する必要があります。SANコントローラを使用してパフォーマンス収集の追加や削除を実行できます。スイッチのコレクションを作成する前に、スイッチにライセンスを付与し、**managedContinuously**状態に維持します。このウィンドウには、ライセンスを受けたファブリックのみが表示されます。

手順

ステップ 1 **[SAN] > [ファブリック（Fabrics）]** を選択します。

ステップ 2 パフォーマンス収集を設定するファブリックの横にあるチェックボックスをオンにします。

ステップ 3 **[アクション（Actions）] > [パフォーマンスの設定（Configure Performance）]**を選択します。

[パフォーマンスデータ収集設定（Performance Data Collection Settings）] ウィンドウが表示されます。

ステップ 4 他のチェックボックスを有効にするには、**[パフォーマンス収集（Performance Collection）]** チェックボックスをオンにします。

ステップ 5 必要な **ISL/NPV リンク**、**ホスト**、**ストレージ**、および **FC イーサネット**を選択するか、**[すべて選択（Select All）]** ボックスを選択して、これらのデータタイプのパフォーマンス収集を有効にします。

a) SAN デバイスの温度データを収集するには、**[設定（Settings）] > [サーバー設定（Server Settings）] > [PM]**を選択します。

b) **[PM]** タブで、**[SAN センサー検出を有効にする（Enable SAN Sensor Discovery）]** および **[SAN スイッチの温度を収集する（Collect Temperature for SAN Switches）]** のチェックボックスをオンにします。

ステップ 6 [Apply] をクリックして、設定を保存します

ステップ 7 確認ダイアログボックスで、**[はい（Yes）]** をクリックしてパフォーマンスコレクタを再起動します。

次のタスク

Nexusダッシュボード ファブリック コントローラ にアップグレードした後、復元された古いパフォーマンスマネージャと高チャートデータを表示するには、ファブリックごとにパフォーマンスマネージャを手動で有効にする必要があります。ただし、古い温度データは復元されません。

アップグレードされたNexusダッシュボード ファブリック コントローラ セットアップで温度データの収集を開始するには、**[設定（Settings）] > [サーバー設定 PM（Server Settings PM）]** タブに移動します。**[LAN スイッチの温度を収集（Collect Temperature for LAN Switches）]** チェックボックスをオンにして、**[保存（Save）]** をクリックします。**[LAN センサー検出を有効にする（Enable LAN Sensor Discovery）]** チェックボックスはデフォルトで有効になっていることに注意してください。

SAN Insights

SAN Insights 機能を使用すると、ファブリック内のフロー分析を設定、モニタリング、および表示できます。SAN コントローラの SAN Insights 機能を使用すると、インターフェイスでヘルス関連のインジケータを可視化できるため、ファブリックの問題をすばやく特定できます。また、ヘルスインジケータにより、ファブリックの問題を理解することができます。SAN Insights 機能は、ホストから LUN へのより包括的なエンドツーエンドのフローベースのデータも提供します。

SAN コントローラは、コンパクトな GPB トランスポートを使用して SAN テレメトリストリーミング（STS）をサポートし、テレメトリのパフォーマンスを向上させ、SAN Insights の全体的な拡張性を向上させます。

SAN Insights のストリーミングの安定性とパフォーマンスについては、SAN コントローラの展開にSAN Insights のサーバープロパティを参照してください。SAN Insights の展開にシステム RAM、vCPU、および SSD が使用されていることを確認します。SAN コントローラとスイッチ間の時刻同期を維持するには、NTP の使用をお勧めします。カウンタ統計を表示するための PM 収集を有効にします。

リリース 12.0.1a から、SAN ITL/ITN フローのポリシーベースのアラーム生成を作成できるようになりました。Web UI から、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラームポリシー（Alarm Policies）]**を選択してポリシーを作成します。

前提条件

- SAN Insights は、仮想データノードと物理ノードでサポートされています。
- SAN Insights 機能は、Nexus Dashboard のアプリノード展開ではサポートされていません。
- Nexus Dashboard の単一ノードおよび 3 ノードの展開は、SAN Insights の展開でサポートされています。
- 11.2(1) より古いバージョンの Cisco SAN Insights を使用して、SAN Insights ストリーミングが KVGPB エンコーディングで設定されている場合、スイッチは、SAN Insights バージョン 11.2(1) 以降でストリーミングを設定している間も、KVGPB エンコーディングでストリーミングを継続します。SAN Insights のコンパクトな GPB ストリーミング設定は、SAN コントローラ 11.2(1) 以降でサポートされています。Compact GPB を使用してストリーミングするには、アップグレード後に SAN Insights を新しく設定する前に、古い KVGPB ストリーミングを無効にします。分析とテレメトリを無効にするには、Cisco SAN コントローラ Web UI で、**[SAN] > [ファブリック（Fabrics）]**を選択し、ファブリックを選択し、**[ア**

クション（**Actions**）] > **[SAN Insights の設定（Configure SAN Insights）]**を選択して、**[次へ（Next）]** をクリックします。[スイッチの設定（Switch Configuration）] 画面で、必要なスイッチを選択し、**[アクション（Actions）]**、>**[分析を無効にする（Disable Analytics）]** の順に選択して、選択したスイッチのすべての分析およびテレメトリ設定をクリアします。

- SAN Insights 機能は、Cisco MDS NX-OS リリース 8.3(1) 以降でサポートされています。

永続的な IP アドレスの設定

SAN コントローラリリース 12.1.1e をインストールまたはアップグレードする前に、Cisco Nexus ダッシュボードで永続的な IP アドレスを設定する必要があります。

Cisco Nexus Dashboard で、サービスに IP プール アドレスが割り当てられていることを確認します。詳細については、『*Cisco Nexus Dashboard User Guide*』の「Cluster Configuration」の項を参照してください。

Note SAN コントローラ導入用に 1 つのノードで SAN Insights を構成するには、SAN Insights 受信者に使用可能な永続的 IP が 1 つ必要です。同様に、SAN コントローラを導入するために 3 つのノードで SAN Insights を構成するには、3 つの使用可能な永続的 IP アドレスが必要です。

Cisco Nexus ダッシュボードで永続的 IP アドレスを設定するには、次の手順を実行します。

Procedure

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[クラスタ設定（Cluster Configuration）]** を選択します。

ステップ 2 [全般（General）] タブの [外部サービスプール（External Service Pools）] カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 SAN コントローラの IP アドレスを設定するには、データサービス IP で、**[IP アドレスの追加（Add IP Address）]** をクリックし、必要な IP アドレスを入力して、**[チェック（check）]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

注意事項と制約事項

- SAN Insights 機能を展開するために、SAN コントローラおよびサポートされているスイッチの時間の設定がローカル NTP サーバーに同期されていることを確認します。
- 適用可能な夏時間の設定は、スイッチと SAN コントローラ全体で一貫している必要があります。

- ストリーミング間隔を変更するには、スイッチからCLIを使用して、インストールされている SAN コントローラのクエリを削除します。SAN コントローラサーバーのプロパティで **san.telemetry.streaming.interval** プロパティを変更します。間隔の許容値は 30 ～ 300 秒です。デフォルト値は 30 秒です。デフォルト値に問題がある場合、または値を増やす場合は、デフォルト値を 60 秒に設定します。デフォルト値は、SAN Insights の設定中に変更できます。**[スイッチの設定ウィザード（Switch Configuration）]**の **[間隔（Interval(s)）]** 列で、ドロップダウンリストから必要な値を選択します。
- スイッチ側のポート サンプリング ウィンドウには、すべてのポートが含まれている必要があります（デフォルト）。
- ISL クエリインストールタイプは、ストレージが接続されているスイッチ（ストレージエッジスイッチ）にのみ使用します。
- ISL クエリインストールタイプの場合、SAN Insights の設定ウィザードで、非 MDS プラットフォームスイッチへのポートチャネル ISL のメンバーであるインターフェイスで分析を有効にすることはできません。
- スイッチベースの FM_Server_PKG ライセンスをインストールした後、SAN Insights の設定ウィザードがインストールされたライセンスを検出するまでに最大 5 分かかる場合があります。

SAN Insights ダッシュボードについては、SAN Insightsを参照してください。

SAN Insights の設定については、SAN Insights の設定を参照してください。

SAN Insights のサーバープロパティ

サーバー設定値を変更するには、Web UI の**[設定（Settings）]** > **[サーバー設定（Server Settings）]** > **[Insights]**に移動します。

（注） サーバーのプロパティを変更する場合は、新しいプロパティ値を使用するように SAN コントローラを再起動してください。

次の表で、フィールド名、説明、およびそのデフォルト値について説明します。

表 *2 : SAN Insights* のサーバープロパティ

フィールド名	説明	デフォルト値
テレメトリページのデフォルトプロトコル scsi/nvme	対応するデータを表示するために、SAN Insights UI ページで必要なデフォルトのプロトコル選択を指定します（SCSI または NVMe）。	SCSI
SAN Insights ECT スレッド数	ECT クエリに使用するスレッドの数を指定します。	4

フィールド名	説明	デフォルト値
最大集計バケットサイズ	集計クエリに使用するバケットの最大数を指定します。	40,000
データテーブルダウンロードサイズ	テーブルダウンロードのレコード数を指定します。	1000
ECT データ制限	ECT データ制限を指定します。	14 （注） ECT データ制限の値は、SAN テレメトリ保持ポリシー（ベースライン/後処理）の値以下である必要があります。
SAN テレメトリ偏差の低しきい値	通常と低の変化点となる値を指定します。	1
SAN テレメトリ偏差中しきい値	低と中の変化点となる値を指定します。	15
SAN テレメトリ偏差の高しきい値	中と高の変化点となる値を指定します。	30
NVMe の SAN テレメトリ偏差の低しきい値	NVMe の通常と低の変化点となる値を指定します。	1
NVMe の SAN テレメトリ偏差中しきい値	NVMe の低と中の変化点となる値を指定します。	2
NVMe の SAN テレメトリ偏差の高しきい値	NVMe の中高間の変化点となる値を指定します。	5
SAN テレメトリトレーニングのタイムフレーム	フロー ECT ベースラインのトレーニングタイムフレームを指定します。	7 日
SAN テレメトリトレーニングのリセットタイムフレーム	日数後に ECT ベースライントレーニングを定期的に再開する期間を指定します。	14 日
SAN テレメトリ保持ポリシー： ベースライン/後処理	保持ポリシー（ベースライン/後処理）を指定します。	14

フィールド名	説明	デフォルト値
SAN テレメトリ保持ポリシー：時間ごとのロールアップ	保持ポリシーを指定します：時間ごとのロールアップ	90
テレメトリギャップリセット間隔	レコード間の最大有効時間ギャップを指定します（ドロップ前）。 時間は秒単位です	750
アクティブな異常キャプチャ	ポストプロセッサごとにアクティブに追跡される異常の最大数を指定します。	500
ベースライントレーニングには NOOP フレームが含まれます	ベースライン学習が noop フレームを参照する必要があるかどうかを指定します。	未選択
ベースライントレーニングには負の偏差が含まれます	ベースライン偏差に負の偏差を含めるかどうかを指定します。	オン
テレメトリギャップリセット間隔を使用する	レコード間の時間ギャップに基づいて使用テレメトリリセットを指定します	オン

次の表では、SAN コントローラのインストールのシステム要件について説明します。

表 *3 : SAN Insights* を使用する *SAN* コントローラに必要なシステムメモリ

ノードタイプ	vCPU の数	メモリ	ストレージ
仮想データノード	32	128 GB	3 TB SSD
物理データノード	40	256 GB	4*2.2 TB HDD、370G SSD、1.5 TB NVMe

表 *4 : SAN Insights* 展開の検証済み制限

展開タイプ	検証済み制限 [1] [2]
Cisco Virtual Nexus Dashboard（1 ノード）	80K ITLs/ITNs
Cisco Physical Nexus Dashboard（1 ノード）	120K ITLs/ITNs
Cisco Virtual Nexus Dashboard（3 ノード）	150K ITLs/ITNs
Cisco Physical Nexus Dashboard（3 ノード）	250K ITLs/ITNs

1 Initiator-Target-LUNs（ITLs）
2 Initiator-Target-Namespace ID（ITNs）

SAN Insights の設定

SAN コントローラリリース 12.0.1a から、ファブリックウィンドウでの構成とは別に、トポロジウィンドウで SAN ファブリックを構成できます。

トポロジウィンドウで、SAN ファブリックを右クリックし、**[SAN Insights の構成（Configure SAN Insights）]** を選択し、手順に従って構成します。

SAN Controller Web UI で SAN Insights を構成するには、次の手順を実行します。

Before you begin

SAN Insights を構成する前に、永続的な IP アドレスを構成していることを確認してください。永続的な IP アドレスの設定を参照してください。

SAN コントローラの SAN Insights 機能が有効になっていることを確認します。**[設定（Settings）]** > **[機能管理（Feature Management）]** を選択し、**[SAN Insights]** チェックボックスをオンにします。

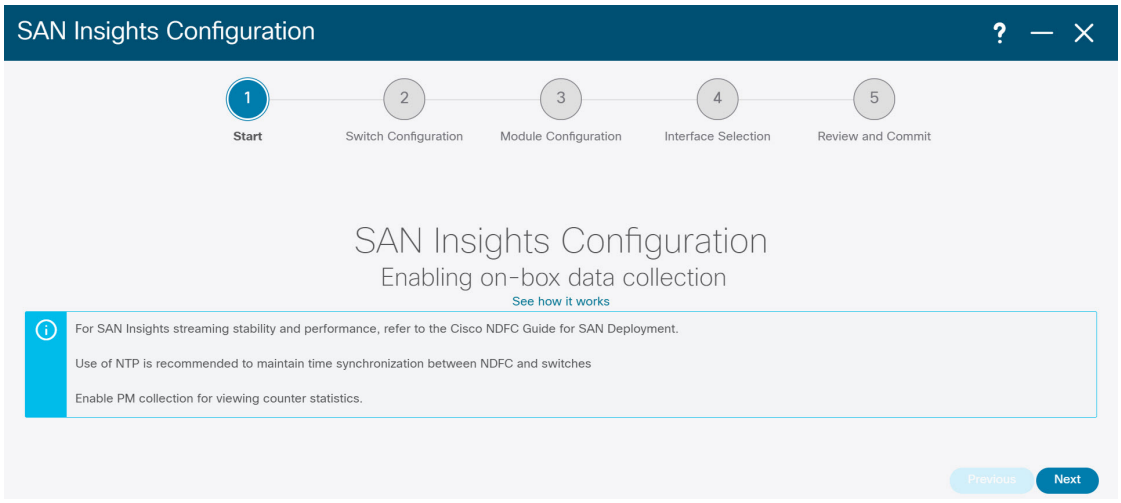
Note 十分なシステム要件と IP アドレスで構成する必要があります。スケール制限の詳細については、SAN Insights のサーバープロパティで、SAN 展開に必要なシステムメモリの表を参照してください。

Procedure

ステップ 1 **[SAN]** > **[ファブリック（Fabrics）]** を選択します。

ステップ 2 必要なファブリックを選択し、**[アクション（Actions）]** > **[SAN Insights の設定（Configure SAN Insights）]** をクリックします。

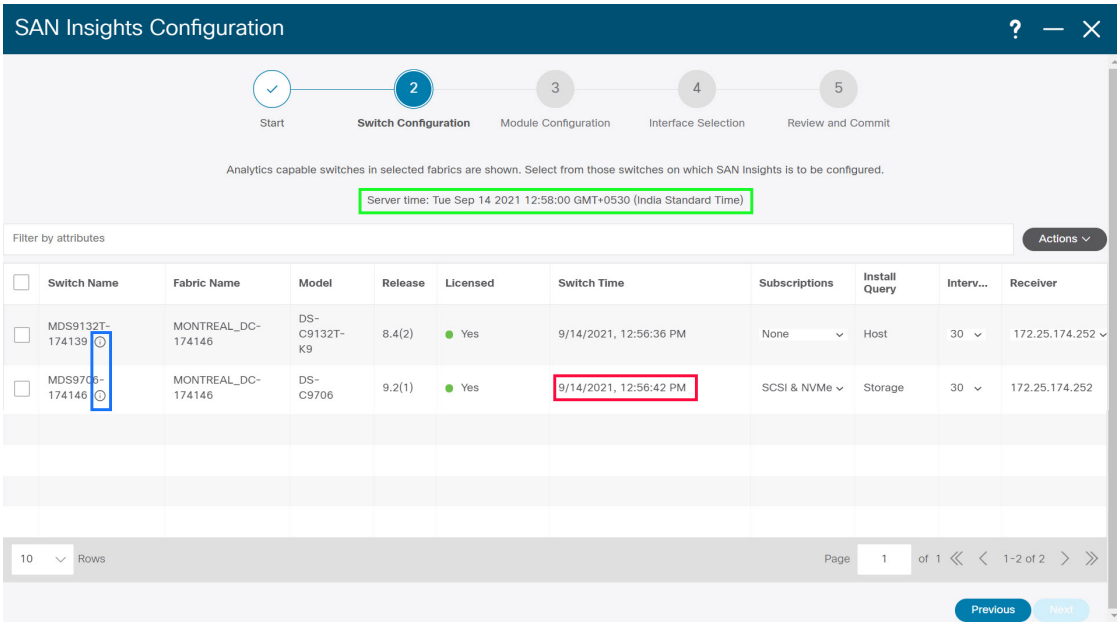
[SAN Insights の設定（SAN Insights Configuration）] ウィザードが表示されます。



ステップ 3 **[SAN Insights の設定（SAN Insights Configuration）]** ウィザードで、**[次へ（Next）]** をクリックします。

[スイッチの設定（Switches Configuration）] ウィザードが表示されます。

ステップ 4 以下に示すようにドロップダウンリストから適切な値を選択した後、SAN Insights 分析とテレメトリストリーミングを構成する必要があるスイッチを選択します。



スイッチに SAN Insights ライセンスがない場合、[ライセンス済み（Licensed）] 列のステータスは **[いいえ（インストールライセンス）（No（install licenses））]** と表示されます。**[ライセンスのインストール（Intall licenses）]** をクリックして、ライセンスをスイッチに適用します。

Note SAN コントローラの時間はこの UI に表示され、スイッチ時間が SAN コントローラの時間とずれていることがわかった場合、スイッチ時間は赤でマークされます。

最後の列で選択された SAN コントローラ受信者の場合、受信者はテレメトリをサブスクライブできます：SCSI のみ、NVMe のみ、SCSI と NVMe の両方、またはなし。これにより、SCSI テレメトリを受信するように 1 つの SAN コントローラサーバーを設定し、NVMe テレメトリを受信するように別の SAN コントローラサーバーを設定できます。

SAN コントローラの展開では、eth0 または eth1 に割り当てられた IP アドレスを使用して、スイッチからの SAN Insights ストリーミングを受信できます。ただし、それぞれのスイッチからの IP 到達可能性を持つ SAN コントローラインターフェイスにストリーミングが設定されていることを確認します。**[受信者（Receiver）]** 列には、検出されたすべてのインターフェイスが一覧表示されます。スイッチから分析データをストリーミングするための SAN コントローラのインストール中に設定された、対応するインターフェイス IP アドレスを選択します。

SAN コントローラをブートストラップするためのファブリックアクセスに管理 IP eth0 とデータ IP eth1 を提供できます。したがって、ストリーミングは、データ IP サブネットで割り当てられた永続的な IP に設定する必要があります。詳細については、永続的な IP アドレスの設定セクションを参照してください。

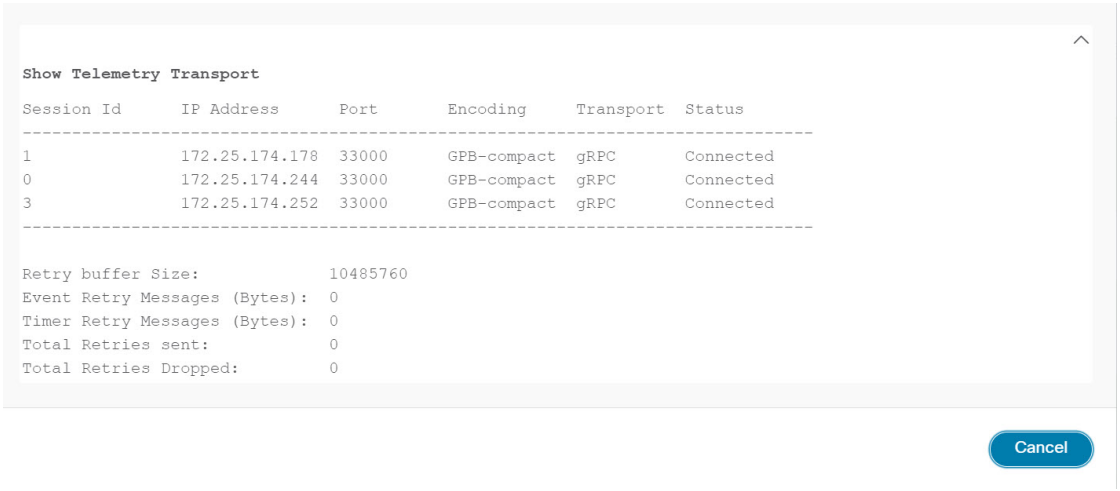
NDFC を仮想 Nexus Dashboard（vND）インスタンス上で実行するには、外部サービス IP アドレスが指定されている Nexus Dashboard インターフェイスに関連付けられているポートグループで無差別モードを有効にする必要があります。 vND は、Nexus Dashboard 管理インターフェイスとデータインターフェイスで構成されています。デフォルトでは、LAN 展開では、Nexus Dashboard 管理インターフェイス サブネットに 2 つの外部サービス IP アドレスが必要です。したがって、関連付けられたポートグループの無差別モードを有効にする必要があります。インバンド管理またはエンドポイントロケータ（EPL）が有効になっている場合は、Nexus Dashboard データ インターフェイス サブネットで外部サービス IP アドレスを指定する必要があります。また、Nexus ダッシュボードデータ/ファブリック インターフェイス ポート グループの無差別モードを有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポート グループに関連付けられた Nexus Dashboard データインターフェイスでのみ有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポート グループに関連付けられた Nexus Dashboard データ インターフェイスでのみ有効にする必要があります。詳細については、*Cisco Nexus ダッシュボード導入ガイド*を参照してください。

同じポートグループで複数の永続的な IP に到達できるように無差別モードを設定するには。詳細については、『*Nexus Dashboard User Guide*』の「*Cluster Configuration*」の項を参照してください。

[サブスクリプション（Subscription）]列では、受信者がサブスクライブするプロトコルを指定できます。ドロップダウンリストから、SCSI、NVMe、両方、またはなしから選択できます。

Note **[サブスクリプション（Subscription）] で [なし（None）]** を選択すると、続行する前に適切なサブスクリプションを選択するよう警告メッセージが表示されます。サブスクリプションに必要なプロトコルを選択します。

[スイッチ名（Switch Name）] 列の **[i]** アイコンをクリックして、スイッチから分析およびテレメトリ機能の設定の詳細を取得できます（分析クエリおよびテレメトリ機能が構成されている場合）。



いずれかのタイプ（dcnminitITL、dcnmtgtITL、dcnmislpcITL、dcnminitITN、dcnmtgtITN、または dcnmislpcITN）の分析クエリがスイッチで設定されていない場合、テレメトリの設定は表示されません。

Note クラスタモードの例に複数の受信者がいる場合は、受信者の横にあるドロップダウンアイコンをクリックして、必要なレシーバーを選択します。

ステップ 5 [次へ（Next）]をクリックします。ストリーミング分析が可能なスイッチは、**[スイッチの選択（Select Switches）]** ページに一覧表示されます。

ステップ 6 SAN Insights を設定する必要があるスイッチを選択します。

Note **[スイッチの選択（Select Switches）]** ページに移動すると、SAN コントローラとスイッチの両方の時間が記録され、表示されます。これは、SAN コントローラとスイッチのクロックが同期していることを確認するのに役立ちます。

単一または複数のスイッチを選択し、**[アクション（Actions）]** > **[分析を無効にする（Disable Analytics）]**の順にクリックして、選択したスイッチのすべての分析およびテレメトリの設定をクリアします。

SAN Insights のコンパクトな GPB ストリーミングの設定がサポートされています。コンパクト GPB を使用してストリーミングするには、アップグレード後に新たに SAN Insights を設定する前に、古い KVGPB ストリーミングを無効にして削除する必要があります。

[クエリのインストール（Install Query）] 列に、スイッチごとのポートのタイプが表示されます。ポートタイプは、**[ISL]**、**[ホスト（host）]**、または**[ストレージ（storage）]**です。

- **[ホスト（host）]**：スイッチ上でホストまたはイニシエータが接続されているすべてのポートを一覧表示します。
- **[ストレージ（storage）]**：スイッチ上でストレージまたはターゲットが接続されているすべてのポートを一覧表示します。
- **[ISL]**：スイッチ上のすべての ISL およびポートチャネル ISL ポートを一覧表示します。
- **[なし（None）]**：クエリがインストールされていないことを示します。

次のクエリが使用されます。

- dcnmtgtITL/dcnmtgtITN：これはストレージのみのクエリです。
- dcnminitITL/dcnminitITN：これはホストのみのクエリです。
- dcnmislpcITL/dcnmislpcITN：これは ISL および pc-member のクエリです。

Note ストレージに接続されているスイッチ（ストレージエッジスイッチ）に ISL クエリインストールタイプを使用する場合は、ISL ベースのクエリを追加する必要があります。

Note SAN コントローラは、重複した ITLs\ITNs を管理しません。ホストクエリとストレージクエリの両方を（ホストとストレージがそれぞれ接続されているスイッチで）設定すると、データは同じ ITL\ITN に対して複製されます。これにより、計算されたメトリックに矛盾が生じます。

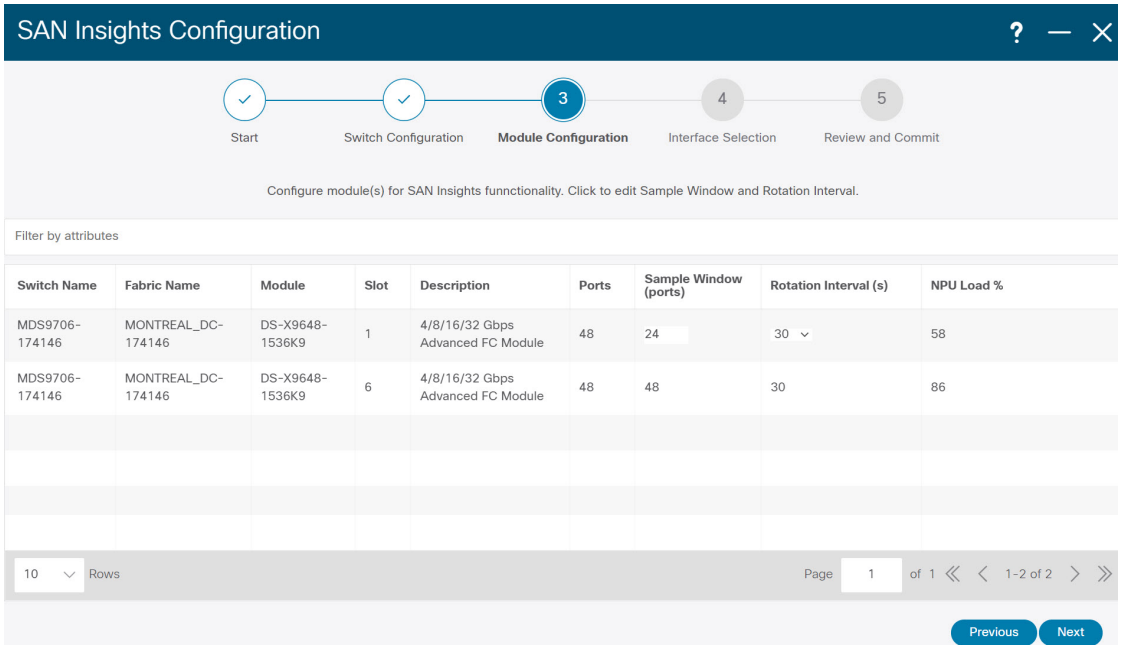
管理者が構成ウィザードで ISL\Host\Storage を選択すると、それぞれのポートがフィルタ処理され、次の手順で一覧表示されます。

ステップ 7 [次へ（Next）] をクリックします。

前のビューで選択したスイッチで分析がサポートされているすべてのモジュールが表示され、最後の列にそれぞれの瞬間的な NPU 負荷が表示されます。このステップでは、モジュールのポートサンプリング構成（オプション）とポートサンプリングのローテーション間隔を指定できます。スイッチのデフォルト設定では、分析のためにスイッチ上のすべての分析対応ポートをモニタリングします。

Note ISL クエリがインストールされている複数の ISL ポートでポートサンプリングが有効になっている場合、メトリックの集計は正確ではありません。すべての交換が同時に利用できるわけではないため、メトリックの集計は正確ではありません。複数の ISL がある ISL クエリでは、ポートサンプリングを使用しないことをお勧めします。

ステップ 8 **[モジュール設定（Module Configuration）]** タブで、SAN Insights 機能のモジュールを設定します。



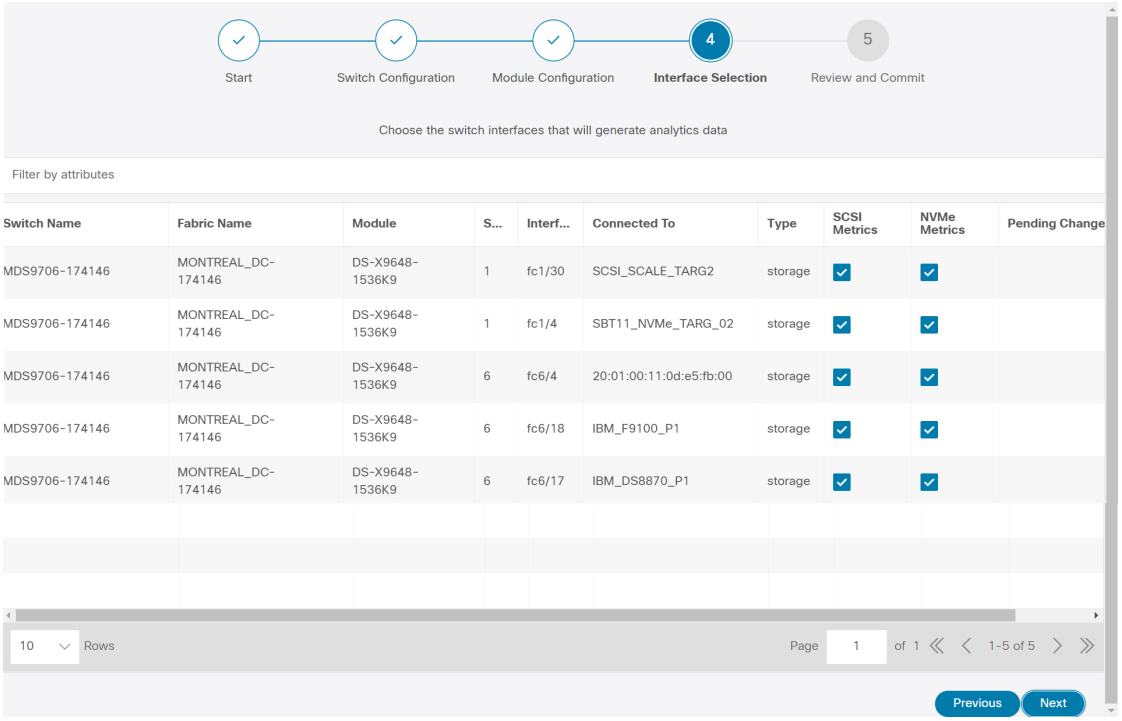
[サンプルウィンドウ（ポート）（Sample Window（ports））]および[ローテーション間隔（秒）（Rotation Interval（seconds））]の値を変更するには、行をクリックして必要な値を入力します。

- 変更を破棄するには、**[キャンセル（Cancel）]** をクリックします。
- 変更を保存するには、**[保存（Save）]** をクリックします。

[NPU ロード（NPU Load）]列には、モジュール内のネットワーク処理ユニット（NPU）が表示されます。

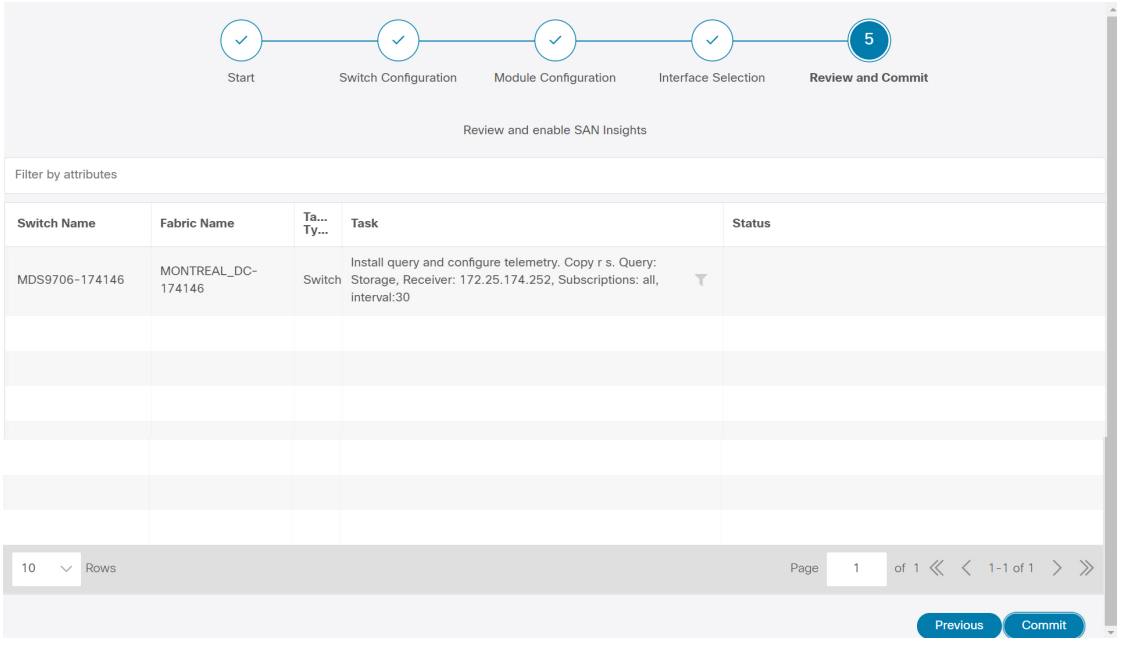
ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 **[インターフェイスの選択（Interface Selection）]** タブで、ファブリック内で分析データを生成するインターフェイスを選択します。



インターフェイスごとに、メトリックを有効化または無効化できます。[SCSI メトリックと NVMe メトリック（SCSI Metrics and NVMe Metrics）] 列のチェックボックスを選択して、目的のポートでの分析を有効または無効にします。

ステップ 11 **[次へ（Next）]** をクリックし、行った変更を確認します。



ステップ 12 [確定する（Commit）] をクリックします。CLI はスイッチで実行されます。

ステップ 13 結果を確認し、応答が成功したことを確認します。

Note 一部の SAN Insights ウィンドウでは、データが表示されるまでに最大 2 時間かかる場合があります。

ステップ 14 **[閉じる（Close）]** をクリックして、ホームページに戻ります。

[閉じる（Close）] アイコンは、スイッチですべての CLI コマンドが実行された後にのみ表示されます。

再度 **[SAN]** > **[ファブリック（Fabrics）]** または [トポロジ（toporogy）] ページに移動して、SAN Insights の設定を変更します。

ファブリック バックアップの構成

選択したファブリックのバックアップを [ファブリック（Fabric）] ウィンドウから設定できます。同様に、**[ファブリックの概要（Fabric Overview）]** ウィンドウでバックアップを設定できます。メイン ウィンドウで **[ファブリックの概要（Fabric Overview）]** > **[アクション（Actions）]** を選択し、**[バックアップの構成（Configure Backup）]** をクリックします。

すべてのファブリック設定とインテントを自動または手動でバックアップできます。インテントである SAN コントローラの設定を保存できます。インテントは、スイッチにプッシュされる場合とされない場合があります。

SAN コントローラは、次のファブリックをバックアップしません。

- モニタ専用モードの外部ファブリック：モニタ専用モードの外部ファブリックのバックアップを作成できますが、復元はできません。外部ファブリックがモニタ専用モードでない場合は、このバックアップを復元できます。
- 親 MSD ファブリック：MSD ファブリックのバックアップを作成できます。親ファブリックからバックアップを開始すると、バックアップ プロセスはメンバー ファブリックにも適用されます。ただし、SAN コントローラは、メンバー ファブリックと MSD ファブリックのすべてのバックアップ情報を 1 つのディレクトリにまとめて保存します。

バックアップされた構成ファイルは、ファブリック名を持つ対応するディレクトリにあります。ファブリックの各バックアップは、手動または自動のどちらでバックアップされたかに関係なく、異なるバージョンとして扱われます。バックアップのすべてのバージョンは、対応するファブリック ディレクトリにあります。

ファブリック設定およびインテントのスケジュール バックアップを有効にできます。

バックアップには、ファブリック上の使用済みリソースに関するリソースマネージャの状態に加えて、インテントとファブリック設定に関連する情報が含まれます。SAN コントローラは、設定プッシュがある場合にのみバックアップされます。SAN コントローラは、最後の設定プッシュ後に手動バックアップをトリガーしなかった場合にのみ、自動バックアップをトリガーします。

ゴールデン バックアップ

アーカイブの制限に達した後でも、削除しないバックアップにマークを付けることができます。これらのバックアップはゴールデン バックアップです。ファブリックのゴールデン バックアップは削除できません。ただし、SAN コントローラは、最大 10 個のゴールデンバックアップのみをアーカイブします。ファブリックの復元中に、バックアップをゴールデン バックアップとしてマークできます。バックアップをゴールデン バックアップとしてマークするには、Web UI から次の手順を実行します。

手順

ステップ 1 ファブリックを選択し、**[Fabrics] > [Fabric Overview] >[Backup]** の順に選択します。

[バックアップ（Backup）] タブが表示されます。

ステップ 2 メイン ウィンドウで、**[アクション（Actions）]** > **[バックアップの構成（Configure Backup）]** を選択します。

[スケジュールされたアーカイブ（Scheduled Archive）] ウィンドウが表示されます。

ステップ 3 バックアップを選択する期間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 バックアップをクリックして、ゴールデンとしてマークするバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[バックアップ（Backup）]** タブから開始します。手動バックアップを開始するには、[バックアップ（Backup）] タブの **[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。

ステップ 5 スイッチウィンドウに移動し、必要なスイッチ名のチェックボックスを選択し、**[スイッチ（Switch）]** > **[スイッチの概要（Switch Overview）]** > **[バックアップ（Backup）]** > **[アクション（Backup Actions）]を選択して、**> **[ゴールデンバックアップとしてマーク（Mark as golden backup）]** を選択します。

確認用のダイアログボックスが表示されます。

ステップ 6 **[はい（Yes）]** をクリックします。

ステップ 7 「ファブリックの復元」の項に記載されている残りのファブリック復元手順を続行するか、ウィンドウを終了します。

ファブリックの概要

ファブリック レベルの **[アクション（Actions）]** ドロップダウン リストでは、バックアップを設定できます。詳細については、ファブリック バックアップの構成 （54 ページ） を参照してください。

[ファブリックの概要（Fabric Overview）] には、ファブリックで次の操作を表示および実行できるタブがあります。

ファブリック サマリ

[ファブリック（Fabric）] をクリックして、サイドキック パネルを開きます。次のセクションでは、ファブリックの概要を表示します。

ヘルス：ファブリックのヘルスを示します。

アラーム：カテゴリに基づいてアラームを表示します。

ファブリック情報：このセクションでは、ファブリックに関する基本情報を提供します。

インベントリ：このセクションでは、スイッチの設定とスイッチの状態に関する情報を提供します。

右上隅にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。

スイッチ

次の表で、**[スイッチ（Switches）]** ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
Fabric Name（ファブリック名）	スイッチに関連付けられているファブリック名を指定します。
ステータス	スイッチのステータスを指定します。

フィールド	説明
ヘルス（Health）	スイッチの正常性ステータスを指定します。正常性ステータスは次のとおりです。 • 正常 • 深刻 • 警告 • OK
Ports	スイッチのポートの合計数を指定します。
使用済みポート	スイッチで使用されるポートの合計数を指定します。
モデル	スイッチ モデルを指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。
リリース	スイッチのリリース番号を指定します。
稼働時間	スイッチアップ時間の詳細を指定します。

次の表に、[アクション（Actions）] メニューのドロップダウンリストで、**[LAN] > [スイッチ（Switch）] > [スイッチ（Switch）]** に表示されるアクションメニューを示します。

アクション項目	説明
Device Manager	必要なスイッチのデバイスマネージャにログインできます。**[デバイスマネージャ（Device Manager）]** ログインウィンドウが表示され、ログイン情報を入力してログインします。 Cisco MDS 9000 Device Manager の説明と使用方法については、デバイスマネージャのヘルプを参照してください。
テクニカル サポート	ログの収集を開始できます。詳細については、テクニカル サポート （70 ページ）を参照してください。
CLI の実行	複数のスイッチで複数の CLI コマンドを実行し、各スイッチの出力を zip 形式のテキストファイルとして収集できます。詳細については、CLI の実行 （71 ページ）を参照してください。

モジュール

SAN コントローラWeb UI からモジュールのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[SAN]**、**[スイッチ（Switch）]**、**[スイッチの概要（Switch Overview）]**、**[モジュール（Modules）]** の順に選択します。同様に、ファブリックの概要ウィンドウで、**[SAN] > [ファブリック（Fabric）] > [ファブリックの概要（Fabric Overview）] > [Modules]** の順に表示できます。

[モジュール（Modules）] タブに、選択した範囲のすべてのスイッチとその詳細のリストが表示されます。

テーブルに必要な情報を表示し、**[属性によるフィルタ（Filter by Attributes）]** に詳細を入力できます。

ステップ 2 次の情報が表示されます。

- **[名前（Name）]** にはモジュール名が表示されます。
- **[モデル（Model）]** にモデル名が表示されます。
- **[シリアル番号（Serial Number）]** 列には、シリアル番号が表示されます。
- **[タイプ（Type）]** 列には、モジュールのタイプが表示されます。
- **Oper. Status** 列には、デバイスの動作状態が表示されます。
- **[スロット（Slot）]** 列には、スロット番号が表示されます。
- **[ハードウェア リビジョン（HW Revision）]** 列には、モジュールのハードウェア バージョンが表示されます。
- **[ソフトウェア リビジョン（Software Revision）]** 列には、モジュールのソフトウェア バージョンが表示されます。
- **[アセット ID（Asset ID）]** カラムには、モジュールのアセット ID が表示されます。

インターフェイスの表示

UI Path: **SAN** > **スイッチ** > **スイッチの概要** > **インターフェイス**

同様に、ファブリック概要ウィンドウでインターフェイスを表示できます。

SAN > **ファブリック** > **ファブリックの概要** > **インターフェイス**

次の表では、**[インターフェイス（Interfaces）]** タブに表示されるフィールドについて説明します。

フィールド	説明
名前	インターフェイス名を指定します。
Admin. ステータス	インターフェイスの管理ステータスを指定します。
Oper. ステータス	インターフェイスの動作ステータスを指定します。
理由	失敗の理由を指定します。
スピード	Gb でインターフェイスの速度を指定します。
モード	インターフェイスのモードを指定します。
スイッチ	スイッチの名前を示します。
VSAN	接続された VSAN の名前を指定します。
接続先	接続の詳細を指定します。
接続先のタイプ	接続のタイプを指定します。
説明	インターフェイスの詳細を指定します。
オーナー	ポートの所有者を指定します。
[ポートグループ（Port Group）]	インターフェイスが接続されているポートグループ番号を指定します。

インベントリタブでさまざまな操作を実行するには、次の手順に従います。

手順

ステップ 1 インターフェイスに対してシャットダウンを実行しない場合は、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]**>**[シャットダウンな（No Shutdown）]** をクリックします。

警告ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

ステップ 2 インターフェイスをシャットダウンするには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]** > **[シャットダウン（Shutdown）]**をクリックします。

警告ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

ステップ 3 インターフェイスのポート所有者を割り当てるには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]** > **[所有者（Owner）]**をクリックします。

ステップ 4 **[ポート所有者の設定（Set Port Owner）]** ウィンドウが表示され、必要な名前を入力して **[適用（Apply）]** をクリックします。

ステップ 5 インターフェイスの診断をリンクするには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）] > [リンク診断（Link Diagnostics）]**をクリックします。

デバイス エイリアス

デバイスエイリアスは、ポート WWN のわかりやすい名前です。デバイスエイリアス名は、ゾーン分割、QoS、ポートセキュリティなどの機能を設定するときに指定できます。デバイスエイリアス アプリケーションは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベースの管理およびファブリック全体への配布を実現します。

次の表では、**[デバイスエイリアス（Device Aliases）]** タブの下に表示されるフィールドについて説明します。

フィールド	説明
スイッチ	デバイスエイリアスイッチ名を表示します。
デバイス エイリアス	スイッチから取得したエイリアスを表示します。
pWWN	ポート WWN を表示します。

この項の内容は、次のとおりです。

デバイスエイリアスの設定

ファブリックテーブルから必要なファブリックをクリックすると、スライドインパネルが表示されます。[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）]** ウィンドウを表示し、[デバイスエイリアス（Device Alias）] タブをクリックします。

デバイスエイリアス設定を実行する前に、CFS タブでステータスをチェックして、ステータスが **[成功（success）]** であることを確認します。

（注） SAN コントローラ Web UI からデバイスエイリアス設定を実行するには、ファブリックをデバイスエイリアス拡張モードとして設定する必要があります。

デバイスエイリアスを追加、編集、または削除するには、次の手順を実行します。

手順

ステップ 1 デバイスエイリアスを追加する必要があるスイッチ列の横にあるチェックボックスをオンにします

a) **[アクション（Actions）] > [デバイスエイリアスの追加（Add device alias）]** をクリックします。

[デバイスエイリアスの追加（Add device alias）] ウィンドウが表示されます。

プロビジョニングされたすべてのポート WWN がテーブルに入力されます。

b) **[デバイスエイリアス（Device Alias）]** フィールドにデバイスエイリアス名を入力して、選択した pWWN のデバイスエイリアスを作成することを示します。
c) **[保存（Save）]** をクリックして、インラインエディタモードを終了します。
d) **[適用（Apply）]** をクリックして、デバイスエイリアスをスイッチに割り当てます。

プロビジョニングされていないポート WWN を使用してデバイスエイリアスを作成することもできます。

a) 事前プロビジョニング デバイス エイリアスの **[+]** アイコンをクリックして、インラインエディタモードで新しいテーブル行を作成します。
b) **[pWWN]** フィールドに、プロビジョニングされていないポートの WWN と、新しいエイリアスのデバイスエイリアスを入力します。
c) **[保存（Save）]** をクリックして、インラインエディタモードを終了します。
d) **[適用（Apply）]** をクリックして、デバイスエイリアスと関連付けられた pWWN をスイッチに割り当てます。

（注） デバイスエイリアスをスイッチに適用する前に [デバイスエイリアスの追加（Add device alias）] ウィンドウを閉じると、変更は破棄され、デバイスエイリアスは作成されません。

ステップ 2 デバイスエイリアスを編集するには、スイッチ列の横にあるチェックボックスをオンにしてから、**[アクション（Actions）] > [デバイスエイリアスの編集（Edit device aliases）]** をクリックします。

（注） 複数のスイッチを選択して、デバイスエイリアスを編集できます。

[デバイスエイリアスの編集（Edit device alias）] ウィンドウが表示されます。

選択したすべてのポート WWN がテーブルに入力されます。

a) [pWWN] 列の横にある **[編集（Edit）]** アイコンをクリックします。
b) [デバイスエイリアス（Device Alias）] フィールドに必要なデバイスエイリアス名を入力し、**[チェックマーク（tick）]** アイコンをクリックして名前を保存します。
c) 同じ手順を繰り返して、他のデバイスエイリアス名を編集します。
d) **[適用（Apply）]** をクリックして、編集したデバイスエイリアスをスイッチに保存します。

（注） デバイスエイリアスの名前を変更すると、デバイスエイリアスを編集するとトラフィックが中断され、ゾーンメンバータイプを確認するよう求める警告メッセージが表示されます。Cisco NX-OS リリースの場合：

- 7.x リリース：7.3(0) リリースより前
- 6.x リリース：6.2(15) リリースより前

e) **[キャンセル（Cancel）]** をクリックして変更内容を破棄するか、または **[確認（Confirm）]** をクリックして変更内容を保存します。

ステップ 3 デバイスエイリアスを削除する必要があるスイッチ列の横にあるチェックボックスをオンにします。

a) **[アクション（Actions）] > [デバイスエイリアスの削除（Delete device alias）]** をクリックします。

確認ウィンドウが表示されます。

（注） デバイスエイリアスを削除すると、トラフィックが中断する可能性があります。

b) **[はい（Yes）]** をクリックして、デバイスエイリアスを削除します。

ステップ 4 サービスプロファイルが添付されたエンドデバイスの場合、サービスプロファイル名が **[デバイスエイリアス（Device Alias）]** フィールドに入力されます。これにより、サービスプロファイル名をそれらのデバイスのデバイスエイリアス名として使用できます。

デバイスエイリアスの作成は、**[適用（Apply）]** をクリックした後に CFS 自動コミットされます。**[CFS]** タブをクリックして、デバイスエイリアスの作成後に CFS が適切に実行されているかどうかを確認します。失敗した場合は、トラブルシューティングを行い、問題を修正する必要があります。

CFS

ファブリック内のすべての適格なスイッチの CFS 情報が一覧表示されます。デバイスエイリアス設定を実行する前に、**CFS** タブでステータスをチェックして、ステータスが [成功（success）] であることを確認します。CFS が別のユーザーによってロックされている場合、または前の操作が失敗した場合は、CFS セッションがロック解除されていることを確認してください。

次の表では、**CFS** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
機能	スイッチの機能を指定します。
直前のアクション	スイッチで最後に実行されたアクションを指定します。
結果	実行されたアクションが成功または失敗であることを指定します。
所有者スイッチのロック	スイッチがロックされているかどうかを指定します。
所有者ユーザーのロック	スイッチがロックされている場合のユーザーロール名を指定します。
結合ステータス	スイッチのマージステータスを指定します。

SAN コントローラ Web UI から CFS 情報を表示するには、次の手順を実行します。

手順

ステップ 1 CFS設定をコミットするには、**スイッチ**オプションボタンを選択し、**コミット**をクリックします。

このスイッチの CFS 設定はコミットされています。

ステップ 2 CFS 設定を中止するには、**スイッチ**オプションボタンを選択し、**中止**をクリックします。

このスイッチの CFS 設定は中止されます。

ステップ 3 CFS設定のロックをクリアするには、**スイッチ**オプションボタンを選択し、**ロックのクリア**をクリックします。

CFS が別のユーザーによってロックされている場合、または前の操作が失敗した場合は、CFS セッションがロック解除されていることを確認してください。

イベント分析

イベント分析には、次のトピックが含まれます。

- アラーム （207 ページ）
- イベント （219 ページ）
- アカウンティング （224 ページ）

バックアップアクションの実行

次の表で、**[バックアップ（Backup）]** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
バックアップ日	バックアップの日付を指定します。
バックアップ タグ	バックアップ名を指定します。
バックアップのタイプ	バックアップ タイプがゴールデン バックアップであるかどうかを指定します。
設定ファイル	設定ファイルを指定します。

次の表では、**[アクション（Action）]** に表示されるフィールドおよび説明について記述します。

アクション	説明
今すぐバックアップ	• **[今すぐバックアップ（Backup now）]** を選択します。 **[バックアップの新規作成（Create new backup）]** ウィンドウが表示されます。 • **[バックアップタグ（Backup tag）]** フィールドに名前を入力します。必要に応じて、**[バックアップをゴールデンとしてマークする（Mark backup as golden）]** チェックボックスをオンにします。 ゴールデンバックアップの詳細については、「ゴールデン バックアップ （55 ページ）」を参照してください。 • [OK] をクリックします。
ブートフラッシュにコピー	**[ブートフラッシュにコピー（Copy to bootflash）]** を選択します。確認ウィンドウが表示されます。[OK] をクリックします。 ブートフラッシュの詳細については、「ブートフラッシュのコピー（83 ページ）」をチェックしてください。
比較	スイッチの設定を比較するために必要なスイッチ名を選択し、**[比較（Compare）]** を選択します。 インスタンスで選択できるスイッチは 2 つだけです。 **[設定の比較（Compare Config）]** ウィンドウが表示され、2 つの設定ファイルの違いが表示されます。 ソースおよびターゲットの設定ファイルの内容は、2 つの列に表示されます。 設定ファイルの違いは、凡例とともに表に示されています。 • **赤**： 削除された設定の詳細。 • **緑**：新しく追加された設定の詳細。 • **青**：変更された設定の詳細。
エクスポート	[Export] をクリックします。 ファイルがローカルシステムにダウンロードされます。サードパーティのファイル転送ツールを使用して、これらのファイルを外部サーバーに転送できます。
タグの編集	**[タグの編集（Edit tag）]** をクリックして、バックアップタグ名を変更します。
ゴールデンとしてマーク	既存のバックアップをゴールデンバックアップとしてマークするには、**[ゴールデンとしてマーク]** を選択します。確認ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

アクション	説明
ゴールデンとして削除	ゴールデンバックアップから既存のバックアップを削除するには、**[ゴールデンとして削除（Remove as gold）]** を選択します。確認ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。
Delete	既存のバックアップを削除するには、**[削除（Delete）]** を選択します。確認ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。 （注） • バックアップをゴールデンバックアップとしてマークしている場合。ゴールデンバックアップが削除されていることを確認してください。そうしないと、既存のバックアップを削除できないというエラーが表示されます。 • 一度に 1 つのバックアップを削除できます。

ポートの使用の表示

[ポートの使用（Port Usage）] タブで次の情報を表示できます。

- **[ポート速度（Port Speed）]** 列にはポートの速度が表示されます。
- **[使用済みポート（Used Ports）]** 列には、前述のポート速度の合計ポートが表示されます。
- **[使用可能なポート（Available Ports）]** 列には、ポート速度で使用可能なポートが表示されます。
- **[ポートの合計（Total Ports）]** 列には、上記の速度のポートの合計が表示されます。
- **[推定残り日数（Estimated Day Left）]** 列には、ポートの推定残り日数が表示されます。

[属性別フィルタ処理（Filter by attribute）] を使用して、必要な情報を表示できます。

表を更新するには、**[更新（Refresh）]** アイコンをクリックします。

[使用済みポート（Used ports）] には、選択したスイッチの使用済みポートの合計が表示されます。**[ポートの合計（Total ports）]** には、選択したスイッチで使用可能なポートの合計が表示されます。

メトリック

[メトリック (Metric)] タブには、インフラストラクチャの正常性とステータスが表示されます。CPU 使用率、メモリ使用率、トラフィック、および温度、の詳細を表示できます。

次の表では、**[CPU]** および **[メモリ (Memory)]** タブでの列の表示について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	スイッチの IP アドレスを指定します。
最小値 (Low Value (%))	スイッチの最小 CPU 使用率の値を示します。
平均値 (Avg. Value (%))	スイッチの平均 CPU 使用率の値を示します。
最大値 (High Value (%))	スイッチの最大 CPU 使用率の値を示します。
範囲プレビュー (Range Preview)	線形範囲のプレビューを示します。
前回の更新時刻	スイッチが最後に更新された日時を表示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

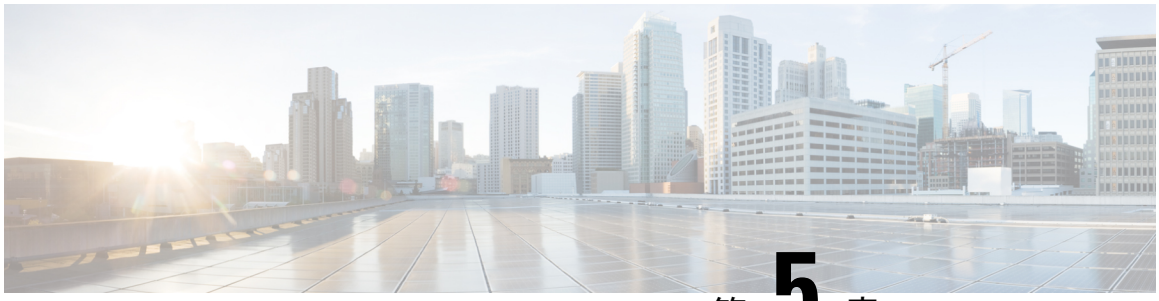
次の表では、**[トラフィック (Traffic)]** タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
平均Rx	平均 Rx 値を示します。
ピーク Rx (Peak Rx)	ピーク Rx 値を示します。
平均Tx	平均 Tx 値を示します。
ピーク Tx (Peak Tx)	ピーク Tx 値を示します。
平均Rx+Tx	Rx および Tx 値の平均を示します。
平均Errors	平均エラー値を示します。
ピーク エラー (Peak Errors)	ピーク エラー値を示します。
平均破棄	平均廃棄値を示します。
ピーク廃棄 (Peak Discards)	ピーク廃棄値を示します。
前回の更新時刻	最後に更新された日時を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

次の表では、**[温度 (Temperature)]**タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	平均 Rx 値を指します。

フィールド	説明
モジュール温度 (Temperature Module)	ピーク Rx 値を指します。
最低値 (Low Value (C))	最低温度の値を示します。
平均値 (Avg. Value (C))	平均温度の値を示します。
最高値 (High Value (C))	最高温度の値を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。



第 5 章

スイッチ

スイッチ

次の表で、**[スイッチ（Switches）]** ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
Fabric Name（ファブリック名）	スイッチに関連付けられているファブリック名を指定します。
ステータス	スイッチのステータスを指定します。
ヘルス（Health）	スイッチの正常性ステータスを指定します。正常性ステータスは次のとおりです。 • 正常 • 深刻 • 警告 • OK
Ports	スイッチのポートの合計数を指定します。
使用済みポート	スイッチで使用されるポートの合計数を指定します。
モデル	スイッチ モデルを指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。

フィールド	説明
リリース	スイッチのリリース番号を指定します。
稼働時間	スイッチアップ時間の詳細を指定します。

次の表に、[アクション（Actions）] メニューのドロップダウンリストで、**[LAN] > [スイッチ（Switch）] > [スイッチ（Switch）]** に表示されるアクションメニューを示します。

アクション項目	説明
Device Manager	必要なスイッチのデバイスマネージャにログインできます。**[デバイスマネージャ（Device Manager）]** ログインウィンドウが表示され、ログイン情報を入力してログインします。 Cisco MDS 9000 Device Manager の説明と使用方法については、デバイスマネージャのヘルプを参照してください。
テクニカル サポート	ログの収集を開始できます。詳細については、テクニカル サポート （70 ページ）を参照してください。
CLI の実行	複数のスイッチで複数の CLI コマンドを実行し、各スイッチの出力を zip 形式のテキストファイルとして収集できます。詳細については、CLI の実行 （71 ページ）を参照してください。

Device Manager

デバイス マネージャ をクリックして Cisco MDS 9000 Device Manager の説明と使用方法を表示してください。

（注） **[スイッチの概要（Switch Overview）]** 画面で別のタブに移動すると、Device Manger セッションが終了します。

テクニカル サポート

[アクション（Actions）] ドロップダウンリストから、**[テクニカルサポート（Tech Support）]** を選択してログ収集を開始します。ウィンドウが表示されます。

- **[セッションタイムアウト（Session timeout）]** フィールドに時間を分単位で入力します。デフォルトの時間は 20 分です。
- **[コマンド（Command）]** テキストフィールドにコマンドを入力し、**[実行（Run）]** をクリックします。

- [データが正常に送信され、テクニカルサポートが開始されました（Data submitted successfully, tech support starting）] という確認ウィンドウが表示され、**[確認（Confirm）]** をクリックしてステータスが **[完了（Completed）]** に変わります。
- レポートをダウンロードするには、**[テクニカルサポートのダウンロード（Download Tech Support）]** をクリックします。

CLI の実行

リリース 12.0.2f 以降 、Cisco NDFC SAN コントローラを使用すると、スイッチで CLI コマンドを実行できます。各スイッチの `.zip` ファイル内の CLI コマンドからの出力を収集できます。

スイッチで CLI コマンドを実行するには、次の手順を実行します。

1. Cisco NDFC UI で、**[SAN] > [スイッチ（Switches）] > [スイッチ（Switches）]** を選択します。
2. CLI コマンドを実行するスイッチを選択します。

   複数のスイッチを選択して、一連の CLI コマンドを同時に実行できます。
3. **[アクション（Actions）]** ドロップダウンリストから、**[CLI の実行（Execute CLI）]** を選択します。

   [スイッチ CLI の実行（Execute Switch CLI）] 画面が表示されます。
4. **[設定（Configure）]** タブで、**[選択されたスイッチ（Selected Switches）]** の下のハイパーリンクをクリックして、CLI が実行される選択されたスイッチを表示します。
5. **[CLI コマンド（CLI Commands）]** テキストボックスに、スイッチで実行する CLI コマンドを入力します。

   1 行に 1 つのコマンドを入力するようにしてください。
6. [実行（Execute）] をクリックします。

   成功（Success） 確認メッセージが表示されます。
7. **[実行（Execute）]** タブで、テーブルには、スイッチ、関連するファブリック、およびCLIの実行ステータスが表示されます。
8. **[出力のダウンロード（Download output）]** をクリックして、コマンド出力をダウンロードします。

（注） CLI 経由でスイッチに到達できない場合、zip ファイルの出力にエラーが表示されます。

拡張されたロールベースのアクセス制御

SAN コントローラリリース 12.0.1(a) からは、すべての RBAC が Nexus ダッシュボードにあります。ユーザロールとアクセスは、NDFC 上のファブリックの Nexus ダッシュボードから定義されます。

Nexusダッシュボードの管理者ロールは、NDFCのネットワーク管理者ロールと見なされます。

DCNM には、さまざまなアクセスと操作を実行するための 5 つのロールがありました。ユーザーがアクセスする場合、ネットワークステージロールを持つファブリックは、ネットワークステージロールとして他のすべてのファブリックにアクセスできます。したがって、ユーザー名は DCNM でのロールによって制限されます。

Cisco NDFC リリース 12.0.1(a) には同じ 5 つのロールがありますが、Nexus ダッシュボードの統合により詳細なRBACを実行できます。ユーザーがネットワークステージロールとしてファブリックにアクセスする場合、同じユーザーは、管理者またはオペレーターロールなどの他のユーザーロールを使用して別のファブリックにアクセスできます。したがって、ユーザーは NDFC のさまざまなファブリックでさまざまなアクセス権を持つことができます。

NDFC RBAC は、次のロールをサポートします。

- NDFC アクセス管理者
- NDFC デバイス アップグレード管理者
- NDFC ネットワーク管理者
- NDFC ネットワーク オペレータ
- NDFC ネットワーク ステージャ

次の表では、NDFC でのユーザーロールとその権限について説明します。

ロール	権限
NDFC アクセス管理者	読み取り/書き込み 参照先
NDFC デバイス アップグレード管理者	読み取り/書き込み
NDFC ネットワーク管理者	読み取り/書き込み
NDFC ネットワーク オペレータ	読み取り
NDFC ネットワーク ステージャ	読み取り/書き込み

DCNM では、下位互換性のために次のロールがサポートされています。

- SAN 管理者（ネットワーク管理者にマッピング）
- グローバル管理者 (ネットワーク管理者にマッピング)
- SAN ネットワーク管理者（ネットワーク管理者にマッピング）

- サーバー管理者（ネットワーク管理者にマッピング）

（注） どのウィンドウでも、ログインしているユーザーロールで実行できないアクションはグレー表示されます。

NDFC ネットワーク管理者

NDFC ネットワーク管理者ロールを持つユーザは、SAN コントローラですべての操作を実行できます。

NDFC ネットワーク管理者ロールを持つユーザーは、 SAN コントローラの特定のファブリックまたはすべてのファブリックをフリーズできます。

NDFC デバイス アップグレード管理者

NDFC デバイス アップグレード管理者ロールを持つユーザは、**[イメージ管理（Image Management）]ウィンドウでのみ操作を実行できます。**

詳細については、「イメージ管理」の項を参照してください。

NDFC アクセス管理者

NDFC アクセス管理者ロールを持つユーザは、すべてのファブリックの**[インターフェイス マネージャ（Interface Manager）]** ウィンドウでのみ操作を実行できます。

NDFC アクセス管理者は、次のアクションを実行できます。

- レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。
- ホスト vPC、およびイーサネット インターフェイスを編集します。
- 管理インターフェイスからの保存、プレビュー、および展開。
- LAN クラシックのインターフェイス、およびポリシーに関連付けられていない場合は外部ファブリックを編集します。

  nve、管理、トンネル、サブインターフェイス、SVI、インターフェイス グループ、およびループバック インターフェイスを除く

ただし、SAN コントローラ アクセス ロールを持つユーザは、次のアクションを実行できません。

- レイヤ 3 ポートチャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。
- レイヤ 3、ST FEX、AA FEX のメンバー インターフェイスおよびポート チャネルは編集できません。
- アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。

- ピア リンク ポート チャネルを編集できません。
- 管理インターフェイスを編集できません。
- トンネルを編集できません。

（注） ファブリックまたはSANコントローラが展開フリーズ モードの場合、このロールのアイコンとボタンはグレー表示されます。

NDFC ネットワーク ステージャ

NDFC ネットワーク ステージャ ロールを持つユーザは、SANコントローラで設定を変更できます。**NDFC ネットワーク管理者**ロールを持つユーザは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

- インターフェイス構成の編集
- ポリシーの表示または編集
- インターフェイスの作成
- ファブリック設定の変更
- テンプレートの編集または作成

ただし、ネットワーク ステージャは次のアクションを実行できません。

- スイッチに設定を展開できません。
- SANコントローラWeb UIまたはREST APIから展開関連のアクションを実行できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。
- メンテナンス モードの切り替えはできません。
- 展開フリーズモードでファブリックを移動したり、展開モードから解放したりすることはできません。
- パッチをインストールします。
- スイッチをアップグレードできません。
- ファブリックを作成または削除できません。
- スイッチをインポートまたは削除できません。

NDFC ネットワーク オペレータ

ネットワーク オペレータは、ファブリック ビルダー、ファブリック設定、構成のプレビュー、ポリシー、およびテンプレートを表示できます。ただし、ネットワーク オペレータは次の操作を実行できません。

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

ネットワーク オペレータとネットワーク ステージャの違いは、ネットワーク ステージャとして、既存のファブリックのインテントのみを定義できますが、それらの設定を展開できないことです。

ネットワーク ステージャロールを持つユーザがステージングした変更および編集を展開できるのは、ネットワーク管理者だけです。

デフォルトの認証ドメインの選択

Nexus ダッシュボードのデフォルトのログイン画面では、認証用のローカルドメインが選択されます。ドロップダウンリストから利用可能なドメインを選択することで、ログイン時にドメインを変更できます。

Nexus ダッシュボードは、ローカルおよびリモート認証をサポートしています。Nexus ダッシュボードのリモート認証プロバイダーには、RADIUS と TACACS が含まれます。認証のサポートの詳細については、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdfを参照してください。

次の表に、DCNM アクセスと NDFC アクセス間の RBAC の比較を示します。

DCNM 11.x	NDFC 12.x
• ユーザーのロールは 1 つです。 • すべての API とリソースは、この 1 つのロールでアクセスされます。	• ユーザーは、セキュリティドメインの Nexus ダッシュボードごとに異なるロールを持つことができます。 • セキュリティドメインには単一の Nexus ダッシュボードが含まれ、各 Nexus ダッシュボードには単一の NDFC ファブリックが含まれます。
DCNM のオプションへのアクセスを無効化または制限することにより、単一のロールがユーザーに関連付けられます。	単一のロールでは、選択したページに特権リソースのみが表示され、NDFC のその他のオプションでは、選択したリソースに関連付けられたセキュリティドメインに基づいて、制限されたアクセスがグレー表示されます。
シェル、ロール、およびオプションのアクセス制約を含む DCNM AV ペア形式。	シェル、ドメインを含む Nexus ダッシュボード AV ペアフォーマット。

DCNM 11.x	NDFC 12.x
展開タイプ LAN、SAN、または PMN に基づいてサポートされるロール。	network-admin、network-operator、device-upg-admin、network-stager、access-admin などのサポートされているロールは NDFC にあります。 下位互換性のためのレガシーロールのサポート。DCNM のネットワーク管理者としての Nexus ダッシュボード管理ロール。

次の表では、DCNM 11.x AV ペアの形式について説明します。

Cisco DCNM Role	RADIUS Cisco-AV-Pair の値	TACACS+ シェル Cisco-AV-Pair ペアの値
network-operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"

次の表では、NDFC 12.x AV ペアの形式について説明します。

ユーザー ロール	AVPair 値
NDFC アクセス管理者	アクセス管理者
NDFC デバイス アップグレード管理者	Device-upg-admin
NDFC ネットワーク管理者	network-admin
NDFC ネットワーク オペレータ	network-operator
NDFC ネットワーク ステージャ	Network-stager

AV ペア文字列の形式は、特定のユーザーに対して読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかによって異なります。通常の文字列にはドメインが含まれており、その後にスラッシュ（/）で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ（|）で区切られています。

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

Nexus Dashboard のセキュリティ ドメイン

ユーザ ログインに関するアクセス制御情報には、ユーザ ID、パスワードなどの認証データが含まれます。認証データに基づいて、リソースに適宜アクセスできます。Nexus ダッシュボードの管理者は、セキュリティ ドメインを作成し、さまざまなリソース タイプ、リソース イン

スタンスをグループ化し、それらをセキュリティドメインにマッピングできます。管理者は各ユーザの AV ペアを定義します。これにより、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限が定義されます。ファブリックを作成すると、Nexus ダッシュボードに同じファブリック名でサイトが作成されます。これらのサイトは、**[Nexusダッシュボード（Nexus Dashboard）] > [サイト（Sites）]**で作成および表示できます。

SAN コントローラ REST API は、この情報を使用して、認可を確認することによってアクションを実行します。

SAN コントローラリリース 11.x からアップグレードすると、各ファブリックは同じ名前の自動生成サイトにマッピングされます。これらすべてのサイトは、Nexus ダッシュボードの**すべて**のセキュリティ ドメインにマッピングされます。

すべてのリソースは、他のドメインに割り当てられたりマッピングされたりする前に、**すべて**のドメインに配置されます。すべてのセキュリティドメインには、Nexus ダッシュボードで使用可能なすべてのセキュリティ ドメインは含まれません。

AV ペア

セキュリティ ドメインのグループと各ドメインの読み取りおよび書き込みロールは、AV ペアを使用して指定されます。管理者は、各ユーザの AV ペアを定義します。AV ペアは、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限を定義します。

AV ペアの形式は次のとおりです。

```
"avpair" :  "shell : domains = security-domain / write-role-1 | write-role-2、security-domain / write-role-1 | write-role2 / read-role-1 | read-role-2 "
```

例 : `"avpair":`

`"shell:domains=all/network-admin/app-user|network-operator"`「`all/admin/`」はユーザをスーパーユーザにするため、`all/admin/` を使用した例を避けるのが最善です。

write ロールには read ロールも含まれます。したがって、`all/network-admin/` と `all/network-admin/network-admin` は同じです。

（注） SAN コントローラ リリース 12.0.1a から、 SAN コントローラリリース11.x で作成した既存の AV ペア形式がサポートされます。ただし、新しい AV ペアを作成する場合は、上記の形式を使用します。shell:domains にスペースが含まれていないことを確認します。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバー上で VSA cisco-AV-pair を使用して、次の形式で Cisco NX-OS デバイスのユーザーロールマッピングを指定できます。

```
shell:roles="roleA roleB …"
```

cisco-AV-pair 属性にロールオプションを指定しなかった場合のデフォルトのユーザーロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-AV-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュリティ ドメインの作成

Cisco Nexus Dashboard からセキュリティ ドメインを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [セキュリティ（Security）]** の順に選択します。
3. **[セキュリティ ドメイン（Security Domain）]** タブに移動する
4. **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。
5. 必要な詳細を入力し、**[作成（Create）]** をクリックします。

ユーザの作成

Cisco Nexus Dashboard からユーザを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [ユーザー（Users）]** の順に選択します。
3. **[ローカル ユーザーの作成（Create Local User）]** をクリックします。
4. 必要な詳細を入力し、**[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。
5. ドロップダウン リストからドメインを選択します。
6. 適切なチェックボックスをオンにして、 SAN コントローラ サービスの読み取りまたは書き込みロールを割り当てます。
7. [保存（Save）] をクリックします。

スイッチの概要

UI パス： **[SAN] > [スイッチ] > [スイッチの概要]**

[スイッチの概要（Switch Overview）] メニューには、次のサブ メニューがあります。

スイッチの概要の表示

[スイッチの概要（Switch Overview）] タブでは、スイッチの概要とともにスイッチに関する情報を表示できます。**[SAN] > [スイッチ（Switches）]** を移動し、必要なスイッチをクリックしま

す。スライドイン ペインが表示されます。**[起動（Launch）]** アイコンをクリックして、**[スイッチの概要（Switch Overview）]** ウィンドウを表示します。

[概要（Summary）] タブに表示されるデフォルトのカードは次のとおりです。

カード	説明
スイッチ情報	名前、正常性ステータス、IP アドレス、モデル、バージョン、その他のスイッチ情報など、スイッチの詳細を表示します。
イベント分析	**重大**、**メジャー**、**マイナー**、および**警告**の重大度を持つイベントを表示します。詳細については、このカードで **[起動（Launch）]** アイコンをクリックして[イベント（events）]タブに移動します。
関連資料	スイッチのリソース使用率をグラフ形式で表示します。
モジュール	モジュールが検出されたスイッチ、モデル名、カウントを表示します。
インターフェイス	スイッチインターフェイスに関する要約情報を表示します。
ポートの使用	ポートインベントリに関する要約情報を表示します。

モジュール

SAN コントローラWeb UI からモジュールのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[SAN]**、**[スイッチ（Switch）]**、**[スイッチの概要（Switch Overview）]**、**[モジュール（Modules）]** の順に選択します。同様に、ファブリックの概要ウィンドウで、**[SAN] > [ファブリック（Fabric）] > [ファブリックの概要（Fabric Overview）] > [Modules]** の順に表示できます。

[モジュール（Modules）] タブに、選択した範囲のすべてのスイッチとその詳細のリストが表示されます。

テーブルに必要な情報を表示し、**[属性によるフィルタ（Filter by Attributes）]** に詳細を入力できます。

ステップ 2 次の情報が表示されます。

- **[名前（Name）]** にはモジュール名が表示されます。
- **[モデル（Model）]** にモデル名が表示されます。
- **[シリアル番号（Serial Number）]** 列には、シリアル番号が表示されます。
- **[タイプ（Type）]** 列には、モジュールのタイプが表示されます。
- **Oper. Status** 列には、デバイスの動作状態が表示されます。
- **[スロット（Slot）]** 列には、スロット番号が表示されます。
- **[ハードウェア リビジョン（HW Revision）]** 列には、モジュールのハードウェア バージョンが表示されます。
- **[ソフトウェア リビジョン（Software Revision）]** 列には、モジュールのソフトウェア バージョンが表示されます。
- **[アセット ID（Asset ID）]** カラムには、モジュールのアセット ID が表示されます。

インターフェイスの表示

UI Path: **SAN** > **スイッチ** > **スイッチの概要** > **インターフェイス**

同様に、ファブリック概要ウィンドウでインターフェイスを表示できます。

SAN > **ファブリック** > **ファブリックの概要** > **インターフェイス**

次の表では、**[インターフェイス（Interfaces）]** タブに表示されるフィールドについて説明します。

フィールド	説明
名前	インターフェイス名を指定します。
Admin. ステータス	インターフェイスの管理ステータスを指定します。
Oper. ステータス	インターフェイスの動作ステータスを指定します。
理由	失敗の理由を指定します。
スピード	Gb でインターフェイスの速度を指定します。
モード	インターフェイスのモードを指定します。
スイッチ	スイッチの名前を示します。
VSAN	接続された VSAN の名前を指定します。
接続先	接続の詳細を指定します。
接続先のタイプ	接続のタイプを指定します。

フィールド	説明
説明	インターフェイスの詳細を指定します。
オーナー	ポートの所有者を指定します。
[ポートグループ（Port Group）]	インターフェイスが接続されているポートグループ番号を指定します。

インベントリタブでさまざまな操作を実行するには、次の手順に従います。

手順

ステップ 1 インターフェイスに対してシャットダウンを実行しない場合は、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]**>**[シャットダウンな（No Shutdown）]** をクリックします。

警告ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

ステップ 2 インターフェイスをシャットダウンするには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]** > **[シャットダウン（Shutdown）]**をクリックします。

警告ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

ステップ 3 インターフェイスのポート所有者を割り当てるには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]** > **[所有者（Owner）]**をクリックします。

ステップ 4 **[ポート所有者の設定（Set Port Owner）]** ウィンドウが表示され、必要な名前を入力して **[適用（Apply）]** をクリックします。

ステップ 5 インターフェイスの診断をリンクするには、必要なインターフェイスのチェックボックス名を選択し、**[アクション（Actions）]** > **[リンク診断（Link Diagnostics）]**をクリックします。

スイッチライセンスの表示

[ライセンス（Licenses）] タブで次の情報を表示できます。

- **[機能（Feature）]** 列には、選択したスイッチの機能名が表示されます。
- **[ステータス（Status）]**列には、ライセンスのステータスが表示されます。ステータスは、**[使用中（In Use）]** または **[未使用（Unused）]** のいずれかになります。
- **[タイプ（Type）]** 列には、ライセンスのタイプが表示されます。
- **[警告（Warnings）]** 列には、ライセンスの猶予期間とその有効期限が表示されます。

[属性別フィルタ処理（Filter by attribute）] を使用して、必要な情報を表示できます。

表を更新するには、**[更新（Refresh）]** アイコンをクリックします。

イベント分析

イベント分析には、次のトピックが含まれます。

- アラーム （207 ページ）
- イベント （219 ページ）
- アカウンティング （224 ページ）

バックアップの表示

[バックアップ（Backup）] タブで次の情報を表示できます。

- **[スイッチ（Switch）]** 列にはスイッチの名前が表示されます。
- **[バックアップ日（Backup Date）]** 列には、バックアップ日が表示されます。
- **[バックアップタグ（Backup Tag）]** 列には、バックアップタグ名が表示されます。
- **[バックアップの種類（Backup Type）]** 列には、バックアップの種類が表示されます。
- **[設定ファイル（Configuration File）]** 列には、そのデバイス用にアーカイブされた設定ファイルが表示されます。

[属性別フィルタ処理（Filter by attribute）] を使用して、必要な情報を表示できます。

表を更新するには、**[更新（Refresh）]** アイコンをクリックします。

次の表では、このタブで実行できるアクションについて説明します。

アクション	説明
ブートフラッシュにコピー	ブートフラッシュのコピー （83 ページ） を参照してください。
比較	設定ファイルの比較を参照してください。
エクスポート	Export Configurationを参照してください。
タグの編集	スイッチのタグを編集するには。必要なスイッチのチェックボックスをオンにし、**[アクション（Actions）]**>**[タグの編集（Edit tag）]**を選択して、**[OK]** をクリックします。

アクション	説明
ゴールデンとしてマーク	スイッチをゴールデンバックアップとしてマークするには。必要なスイッチのチェックボックスをオンにし、**[アクション（Actions）] > [ゴールデンとしてマーク（Mark as golden）]** を選択します。確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックします。 詳細については、「ゴールデンバックアップ」の項を参照してください。
ゴールデンとして削除	ゴールデンバックアップからスイッチを削除するには。必要なスイッチのチェックボックスをオンにし、**[アクション（Actions）]>[ゴールデンとして削除（Remove as golden）]**を選択します。確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックします。
Delete	バックアップからスイッチを削除するには。必要なスイッチのチェックボックスをオンにし、**[アクション（Actions）]>[削除（Delete）]** を選択します。確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックします。

この項の内容は、次のとおりです。

ブートフラッシュのコピー

設定ファイルは、同じデバイス、別のデバイス、または複数のデバイスに同時にコピーできます。

タスクのステータスを表示するには、次のタスクを実行します。

手順

ステップ 1 SAN コントローラのホームページから、**[SAN] > [スイッチ（Switch）] > [スイッチの概要（Switch Overview）] > [バックアップ（Backup）]** を選択します。

ステップ 2 **[ブートフラッシュにコピー（Copy to bootflash）]** をクリックします。

[ブートフラッシュにコピー（Copy to bootflash）]ページが表示され、**[送信元設定のプレビュー（Source Configuration Preview）]** エリアおよび **[選択したデバイス（Selected Devices）]** エリアが表示されます。

[送信元のプレビュー（Source Preview）]エリアには、デバイスにコピーされた実行/起動/バージョン設定ファイルの内容が表示されます。

ステップ 3 **[選択されたデバイス（Selected Devices）]** エリアで、デバイス名のチェックボックスをオンにして、設定をデバイスにコピーします。

（注） 複数の接続先デバイスを選択して、設定をコピーできます。

選択されたデバイスエリアには、次のフィールドが表示されます。

- [デバイス名（Device Name）]：送信元設定のコピー先のターゲットデバイス名を指定します。
- [IP アドレス（IP Address）]：接続先デバイスの IP アドレスを指定します。
- [グループ（Groups）]：デバイスが属しているグループ。
- [ステータス（Status）]：デバイスのステータスを示します。

ステップ 4 [コピー（Copy）] をクリックします。

確認ウィンドウが表示されます。

ステップ 5 **[はい（Yes）]** をクリックして、設定を接続先デバイス設定にコピーします。

設定ファイルの比較

この機能を使用すると、設定ファイルを同じデバイスの別のバージョンまたは別のデバイスの設定ファイルと比較できます。

設定ファイルを比較するには、次のタスクを実行します。

手順

ステップ 1 チェックボックスをオンにして、比較する 2 つの設定ファイルを選択します。

選択した最初のファイルはソースとして指定され、2 番目の設定ファイルはターゲットファイルとして指定されます。

ステップ 2 **[SAN] > [スイッチ（Switch）] > [スイッチの概要（Switch Overview）] > [比較（Compare）]** に移動します。

ステップ 3 **[設定の比較（Compare Configuration）]** をクリックします。

[設定の差分の表示（View Config Diff）] ページが表示され、2 つの設定ファイルの違いが表示されます。

ソースおよびターゲットの設定ファイルの内容は、2 つの列に表示されます。右上隅のドロップダウンリストから**[すべて（All）]** を選択して、設定全体を表示します。**[変更済み（Changed）]** を選択して、設定ファイルの設定の違いを表示することもできます。

設定ファイルの違いは、凡例とともに表に示されています。

- **[赤（Red）]**： 差分設定の詳細。

- **緑**：新しく追加された設定の詳細。
- **青**：変更された設定の詳細。

ステップ 4 **[ターゲットにコピー（Copy to Target）]** をクリックして、送信元設定をターゲット設定ファイルにコピーします。**[キャンセル（Cancel）]** をクリックして、[設定の詳細（configuration details）] ページに戻ります。

[設定のコピー（Copy Configuration）] ウィンドウには、送信元設定のプレビューと接続先設定のターゲットデバイスが表示されます。選択されたデバイスエリアには、次のフィールドが表示されます。

- [デバイス名（Device Name）]：送信元設定のコピー先のターゲットデバイス名を指定します。
- [IP アドレス（IP Address）]：接続先デバイスの IP アドレスを指定します。
- [グループ（Groups）]：デバイスが属しているグループ。
- [適切な設定（Golden Config）]：接続先設定のバージョンを指定します。
- [ステータス（Status）]：デバイスのステータスを示します。

ステップ 5 **[はい（Yes）]** をクリックして、設定を接続先デバイス設定にコピーします。

Export Configuration

SAN コントローラ サーバーから設定ファイルをエクスポートできます。設定ファイルをエクスポートするには、次のタスクを実行します。

手順

ステップ 1 SAN コントローラのホームページから、**[設定（Configure）] > [バックアップ（Backup）]** を選択し、エクスポートする設定を選択します。

ステップ 2 **[Export Configuration]**をクリックします。

ファイルがローカルシステムにダウンロードされます。サードパーティのファイル転送ツールを使用して、これらのファイルを外部サーバーに転送できます。

ポートの使用の表示

[ポートの使用（Port Usage）] タブで次の情報を表示できます。

- **[ポート速度（Port Speed）]** 列にはポートの速度が表示されます。
- **[使用済みポート（Used Ports）]** 列には、前述のポート速度の合計ポートが表示されます。

- **[使用可能なポート（Available Ports）]** 列には、ポート速度で使用可能なポートが表示されます。
- **[ポートの合計（Total Ports）]** 列には、上記の速度のポートの合計が表示されます。
- **[推定残り日数（Estimated Day Left）]** 列には、ポートの推定残り日数が表示されます。

[属性別フィルタ処理（Filter by attribute）] を使用して、必要な情報を表示できます。

表を更新するには、**[更新（Refresh）]** アイコンをクリックします。

[使用済みポート（Used ports）] には、選択したスイッチの使用済みポートの合計が表示されます。**[ポートの合計（Total ports）]** には、選択したスイッチで使用可能なポートの合計が表示されます。

ブートフラッシュの表示

[ブートフラッシュ（Bootflash）] タブで次の情報を表示できます。

- **[プライマリ ブートフラッシュ サマリ（Primary Bootflash Summary）]** カードには、合計、使用済み、および使用可能な領域が表示されます。
- **[セカンダリ ブートフラッシュ サマリ（Secondary Bootflash Summary）]** カードには、合計、使用済み、および使用可能な領域が表示されます。
- **[ディレクトリ リスト（Directory List）]** 領域に、**プライマリ ブートフラッシュ**と**セカンダリ ブートフラッシュ**のチェックボックスが表示されます。

  この領域には、スイッチのブートフラッシュ上のすべてのファイルとディレクトリのファイル名、サイズ、および最終変更日が表示されます。**[アクション（Actions）] > [削除（Delete）]**を順に選択してファイルを削除し、スイッチで使用可能なスペースを増やします。

Device Manager

デバイス マネージャ をクリックして Cisco MDS 9000 Device Manager の説明と使用方法を表示してください。

（注） **[スイッチの概要（Switch Overview）]** 画面で別のタブに移動すると、Device Manger セッションが終了します。

ブレード

UCS スイッチのインターフェイスは、SAN コントローラ Web UI で、**[SAN] > [スイッチ（Switches）] > [スイッチの概要（Switch Overview）]** から表示できます。

（注） UCS スイッチが SAN コントローラに一覧表示されており、これらのスイッチのステータスが正しいことを確認します。これらのタブは、UCS スイッチについてのみ表示できます。

[ブレード（Blades）] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。

UCS には次の 3 つのタブがあります。

- ブレード
- vNIC
- vHBA

[ブレード（blades）] タブには、すべてのブレード情報がカードとして表示されます。各ブレードエリアの **[詳細（More Details）]** アイコンをクリックして、選択したブレードのサイドパネルに詳細を表示します。

[すべて折りたたむ（Collapse All）] または **[すべて展開（Expand All）]** アイコンをクリックして、すべてのブレードエリアをそれぞれ折りたたむか、すべて展開することができます。

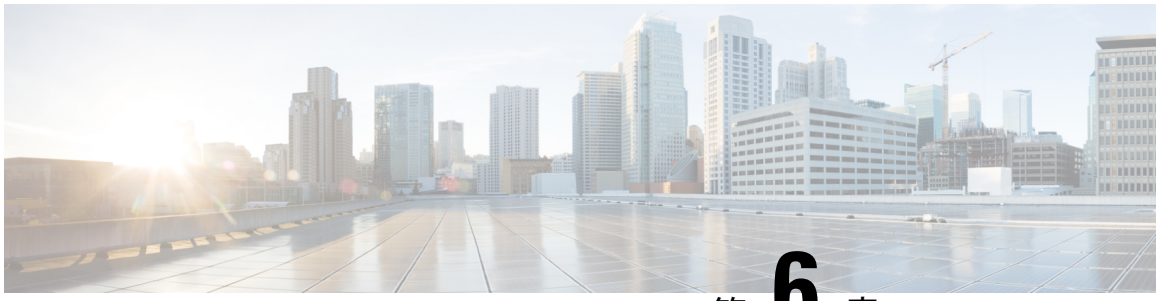
[ブレード（Blades）] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。冗長セットアップのプライマリ UCS FI またはスタンドアロン UCS FI のみが表示されます。

vNIC

[vNICs] タブには、その UCS FI の vNIC のリストが表示されます。グラフアイコンをクリックすると、vNIC の 24 時間のトラフィックが表示されます。

vHBA

[vHBA] タブには、その特定の UCS FI の vHBA のリストが表示されます。グラフアイコンをクリックして、vHBA の 24 時間のトラフィックを表示します。



第 6 章

SAN リンク

SAN リンク

Cisco SAN コントローラを使用すると、SAN ファブリックで FCIP、ポートチャネルを設定できます。Cisco Web Nexusダッシュボード ファブリック コントローラ UI から ISL トラフィックとエラーをモニタリングし、NPV リンクのパフォーマンスを表示することもできます。

ここでは、次の内容について説明します。

ISL およびポートチャネル

ISL トラフィックとエラーウィンドウが表示されます。この表は、SAN ファブリック設定された ISL とポートチャネルを示しています。ドロップダウンを使用して、24 時間、週、月、および年でビューをフィルタ処理できます。

[名前（Name）] 列のトレンドアイコンをクリックして、グラフィカルな表現を表示します。

[アクション（Actions）] ドロップダウンリストから、次の操作を実行できます。

FCIP の設定

FCIP を設定するには、次の手順を実行します。

手順

ステップ 1 **[アクション（Actions）]** ドロップダウンリストから **[FCIP の設定（Configure FCIP）]** を選択します。

このページには、FCIP ウィザードを使用して FCIP を設定するためのタスクが表示されます。

（注） FCIP は、Cisco MDS 9000 24/10-Port SAN 拡張モジュールではサポートされていません。

ステップ 2 **[スイッチペアの選択（Select Switch Pair）]** 画面で、FCIP 経由で接続する 2 つの MDS スイッチをドロップダウンリストから選択します。

各スイッチが正しく機能するには、IP ネットワークに接続されたイーサネットポートが必要です。注フェデレーションセットアップの場合、両方のスイッチは、同じサーバーによって検出または管理されるファブリックに属している必要があります。

ステップ 3 **[次へ（Next）]** をクリックして、イーサネットポートを選択します。

ステップ 4 選択したスイッチ間の FCIP ISL で使用する**イーサネットポート**を選択します。

正常に機能するには、ダウンポートを有効にする必要があります。未設定の 14+2、18+4、9250i、および SSN16 イーサネットポートにセキュリティを適用できます。

ステップ 5 イーサネットポートの IP アドレスを入力し、ポートアドレスが別のサブネットにある場合は IP ルートを指定します。

（注） **[次へ（Next）]** をクリックして、変更を IP アドレスと IP ルートに適用します。

ステップ 6 **[次へ（Next）]** をクリックして、トンネルのプロパティを指定します。

ステップ 7 TCP 接続をトンネリングするには、次のパラメータを指定します。

パラメータを入力します。

- **[最大帯域幅（Max Bandwidth）]** : 1 ～ 10000 の数値を入力します。単位は **[Mb]** です。
- **[最小帯域幅（Min Bandwidth）]** : 最小帯域幅の値を入力します。単位は **[Mb]** です。
- **[推定 RTT（ラウンドトリップ時間）]** : 0 ～ 300000 の数値を入力します。単位は **[us]** です。**[測定（Measure）]** をクリックして、ラウンドトリップ時間を測定します。
- **[書き込みアクセラレーション（Write Acceleration）]** : チェックボックスをオンにして、書き込みアクセラレーションをイネーブルにします。

  （注） 書き込みアクセラレーションが有効になっている場合は、フローが複数の ISL 間で負荷分散しないようにします。

- **[最適な圧縮をイネーブルにする（Enable Optimum Compression）]** チェックボックスをオンにして、最適な圧縮をイネーブルにします。
- **[XRC エミュレータをイネーブルにする（Enable XRC Emulator）]** チェックボックスをオンにして、XRC エミュレータをイネーブルにします。
- **[接続数（Connections）]** : 0 から 100 までの接続数を入力します。

ステップ 8 **[次へ（Next）]** をクリックして、FCIP ISL を作成します。

ステップ 9 スイッチペアの**[プロファイル ID（Profile ID）]** と**[トンネル ID（Tunnel ID）]** を入力し、ドロップダウンリストから **[FICON ポートアドレス（FICON Port Address）]** を選択します。

ステップ 10 **[設定の表示（View Configured）]** をクリックして、**[プロファイル（Profiles）]**と**[トンネル（Tunnels）]**の情報を表示します。

ステップ 11 トランクモード（**Trunk Mode**）を **[非トランク（non-Trunk）]**、**[トランク（trunk）]**、**[自動（auto）]** から選択します。**[Port VSAN（Port VSAN）]** を **[非トランク（non-Trunk）]** および **[自動（auto）]** に指定し、許可 **VSAN リスト（VSAN List**）をトランクトンネルに指定します。

ステップ 12 **[次へ（Next）]** をクリックして最後の [概要（Summary）] ページを表示します。

[概要（Summary）] ビューには、前の手順で選択したものが表示されます。

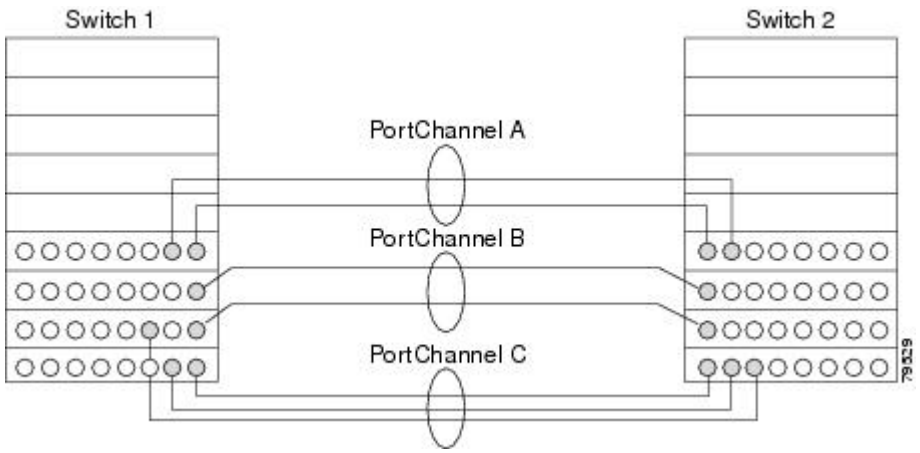
ステップ 13 **[終了（Finish）]** をクリックして FCIP を設定します。

ポート チャネル

ポートチャネルの概要

ポートチャネルは、複数の物理インターフェイスを1つの論理インターフェイスに集約し、より精度の高い集約帯域幅、ロードバランシング、およびリンク冗長性を提供する機能です（下図を参照）。ポートチャネルはスイッチングモジュール間のインターフェイスに接続することができるため、スイッチングモジュールで障害が発生してもポートチャネルのリンクがダウンすることはありません。

図 *1*：ポートチャネルの柔軟性



Cisco MDS 9000 ファミリスイッチのポートチャネルは柔軟に設定できます。これは、3 つの可能なポートチャネル設定を示しています。

- ポートチャネル A は、接続の両端が同一のスイッチングモジュール上にある、2 つのインターフェイスの 2 つのリンクを集約します。
- ポートチャネル B も 2 つのリンクを集約しますが、各リンクは別々のスイッチングモジュールに接続されています。スイッチングモジュールがダウンしても、トラフィックは影響されません。
- ポートチャネル C は 3 つのリンクを集約します。そのうち 2 つのリンクは両端が同一のスイッチングモジュール上にあり、1 つのリンクはスイッチ 1 で別々のスイッチングモジュールに接続されています。

ポートチャネルおよびトランキング

トランキングは、ストレージ業界で一般的に使用されている用語です。ただし、Cisco NX-OS ソフトウェアおよび Cisco MDS 9000 ファミリ スイッチでは、トランキングとポートチャネルを次のように実装します。

- ポートチャネルでは、複数の物理リンクを 1 つの集約論理リンクに組み合わせることができます。
- トランキングでは、EISL 形式のフレームを送信しているリンクで複数の VSAN トラフィックを伝送（トランク）できます。たとえば、E ポートでトランキングを動作させると、その E ポートは TE ポートになります。TE ポートは、Cisco MDS 9000 ファミリ スイッチ特有のものです。業界標準の E ポートは他のベンダーのスイッチにリンクでき、非トランキングインターフェイスと呼ばれます（図 2 : トランキングだけ （92 ページ） および 図 3 : ポートチャネルおよびトランキング （92 ページ） を参照）。

図 *2*: トランキングだけ

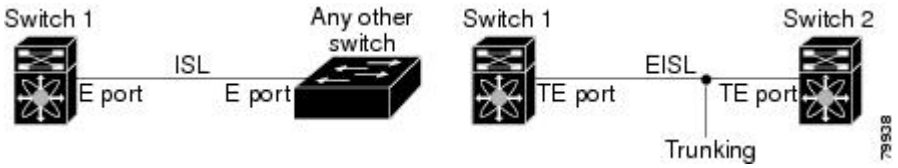
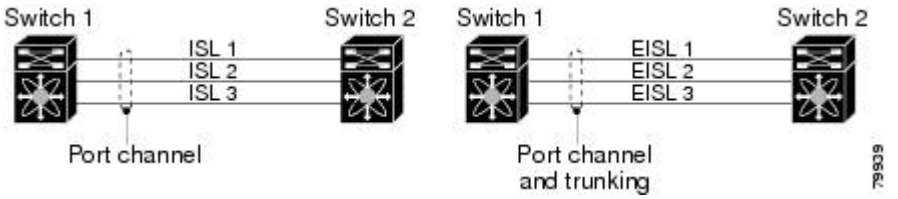


図 *3*: ポートチャネルおよびトランキング



ポートチャネルとトランキングは、ISL で別々に使用されます。

- ポートチャネル：次のポートの組み合わせの間でインターフェイスをチャネリングできます。
  - E ポートおよび TE ポート
  - F ポートおよび NP ポート
  - TF ポートおよび TNP ポート
- トランキング：トランキングでは、スイッチ間で複数の VSAN のトラフィックが伝送されます。
- TE ポート間では、EISL でポートチャネルとトランキングを使用できます。

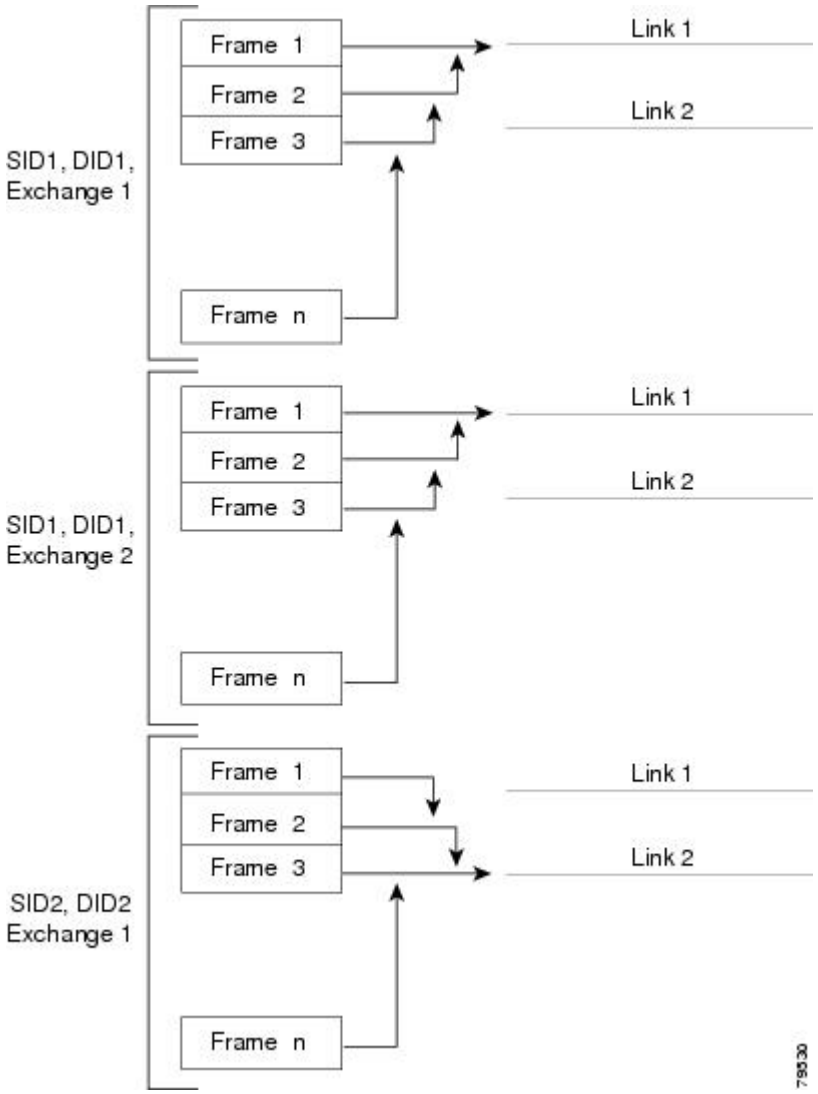
ロード バランシング

次の 2 つの方法でロードバランシング機能がサポートされます。

- フローベース：送信元と接続先間のすべてのフレームが所定のフローで同一のリンクをたどります。つまり、フローの最初のエクスチェンジで選択されたリンクが、後続のすべてのエクスチェンジで使用されます。
- エクスチェンジベース：エクスチェンジの最初のフレームがリンクを選択し、エクスチェンジのその後のフレームは同じリンクを流れます。ただし、後続のエクスチェンジは、別のリンクを使用できます。これにより、やり取りごとにフレームの順序を維持しながら、より細かいロード バランシングが可能になります。

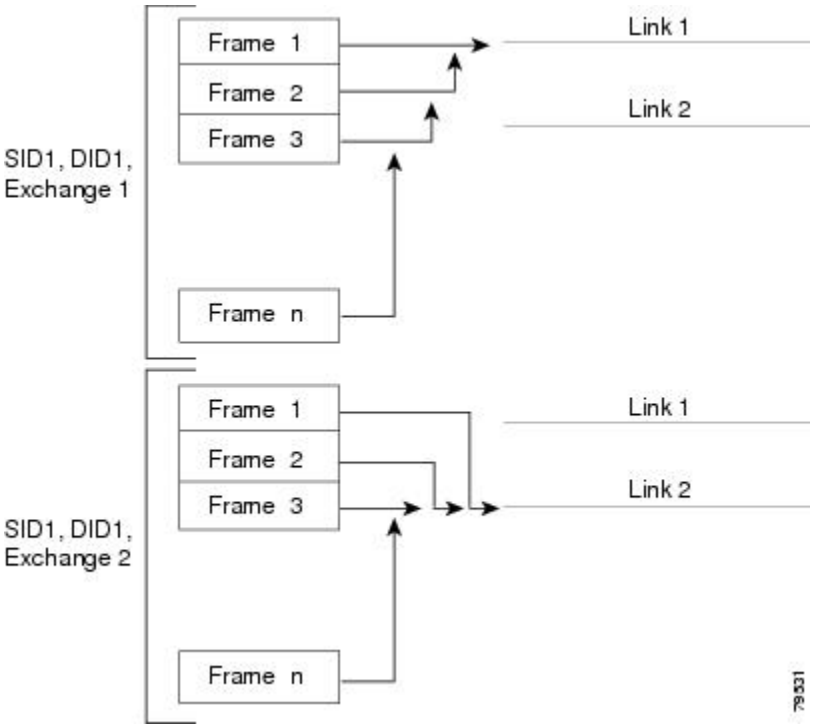
次の図に、 送信元 ID 1（SID1）と接続先 ID1（DID1）を基準とするロードバランシングの動作を示します。フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択されます。そのフローの各後続のフレームが、同一のリンク上に送信されます。SID1 および DID1 のフレームは、リンク 2 を使用しません。

図 *4 : SID1* および *DID1* を基準としたロードバランシング



次の図は、エクスチェンジベースのロードバランシングがどのように機能するかを示しています。エクスチェンジで最初のフレームが転送用にインターフェイスで受信されると、リンク 1 がハッシュ アルゴリズムによって選択されます。その特定のエクスチェンジにある残りすべてのフレームが同一のリンクに送信されます。エクスチェンジ 1 では、リンク 2 を使用するフレームはありません。次のエクスチェンジでは、ハッシュ アルゴリズムによってリンク 2 が選択されます。ここではエクスチェンジ 2 のすべてのフレームが、リンク 2 を使用します。

図 *5 : SID1*、*DID1*、およびエクスチェンジベースのロードバランシング



ポートチャネルモード

チャネルグループのモードパラメータで各ポートチャネルを設定し、このチャネルグループのすべてのメンバーポートでポートチャネルプロトコル動作を決めることができます。チャネルグループ モードに指定できる値は、次のとおりです。

- ON（デフォルト）：メンバーポートはポートチャネルの一部として動作するか、非アクティブになります。このモードでは、ポートチャネルプロトコルは起動されません。ただし、ポート チャネル プロトコル フレームをピアポートから受信した場合、ソフトウェアはネゴシエーション不能ステータスを示します。このモードには、チャネルグループモードが暗黙的に ON になっている Release 2.0(1b) 以前で、既存のポートチャネルの実装と下位互換性があります。4763 Cisco MDS SAN-OS Release 1.3 以前で使用可能なポートチャネルモードは ON モードだけです。オンモードで設定されたポートチャネルでは、ポートチャネルの設定に対してポートの追加または削除を行う場合、各端のポートチャネル メンバーポートを明示的にイネーブルおよびディセーブルに設定する必要があります。また、ローカル ポートおよびリモート ポートが相互に接続されていることを物理的に確認する必要があります。

- ACTIVE：ピアポートのチャネルグループモードに関係なく、メンバーポートはピアポートとポート チャネル プロトコル ネゴシエーションを始めます。チャネルグループで設定されているピアポートがポートチャネルプロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオンモードの動作に設定されます。ACTIVEポートチャネルモードでは、片側でポートチャネルメンバーのポートの有効化および無効化を明示的に行わなくても、自動回復が可能です。

次の表は、ON モードと ACTIVE モードを比較したものです。

表 *5:* チャネルグループ設定の相違点

ON モード	ACTIVE モード
プロトコルは交換されません。	ピアポートとポート チャネル プロトコル ネゴシエーションを行います。
動作値にポートチャネルとの互換性がない場合、インターフェイスは中断状態になります。	動作値にポートチャネルとの互換性がない場合、インターフェイスは分離状態になります。
ポート チャネル メンバー ポート設定の追加または変更を行うとき、片側のポート チャネル メンバー ポートのディセーブル化（shut）およびイネーブル化（no shut）を明示的に行う必要があります。	ポートチャネルインターフェイスを追加または変更すると、SANポートチャネルは自動的に復旧します。
ポートの起動は同期化されません。	すべてのピア スイッチで、チャネル内のすべてのポートの起動が同時に行われます。
プロトコルが交換されないため、すべての誤設定が検出される訳ではありません。	ポートチャネルプロトコルが使用され、誤設定が確実に検出されます。
誤設定ポートを中断ステートに移行します。各端でメンバ ポートを明示的にディセーブル（shut）およびイネーブル（no shut）に設定する必要があります。	誤設定を修正するために、誤設定ポートを隔離ステートに移行します。誤設定を修正すれば、プロトコルによって自動的に復旧されます。

ポートチャネルの削除

ポートチャネルを削除すると、対応するチャネルメンバーシップも削除されます。削除したポートチャネルのすべてのインターフェイスは、個別の物理リンクに変換されます。ポートチャネルの削除後、使用するモード（ACTIVE および ON）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

あるポートのポートチャネルを削除すると、削除したポートチャネル内の各ポートは互換性のあるパラメータ設定（速度、モード、ポートVSAN、許可されているVSAN、ポートセキュリティ）を維持します。これらの設定は、必要に応じて、明示的に変更できます。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブモードを使用する場合、ポートチャネルポートは削除から自動的に回復します。

ポートチャネルのインターフェイス

既存ポートチャネルで物理インターフェイス（またはある範囲のインターフェイス）の追加または削除を行うことができます。設定で互換性があるパラメータはポートチャネルにマッピングされます。ポートチャネルにインターフェイスを追加すると、ポートチャネルのチャネルサイズおよび帯域幅が増加します。ポートチャネルからインターフェイスを削除すると、ポートチャネルのチャネルサイズおよび帯域幅が減少します。

ここでは、ポートチャネルのインターフェイス設定について説明します。ここで説明する内容は、次のとおりです。

ポートチャネルへのインターフェイスの追加

既存ポートチャネルに物理インターフェイス（またはある範囲のインターフェイス）を追加できます。設定で互換性があるパラメータはポートチャネルにマッピングされます。ポートチャネルにインターフェイスを追加すると、ポートチャネルのチャネルサイズおよび帯域幅が増加します。

ポートとポートチャネルで次の構成が同じ場合にのみ、ポートを静的ポートチャネルのメンバーとして構成できます。

- スピード
- モード
- レート モード
- ポート VSAN
- トランキング モード
- 許可 VSAN リストまたは VF-ID リスト

メンバーの追加後、使用するモード（ACTIVE および ON）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します（12 ページの「第 1 世代ポートチャネルの制限事項」セクションを参照）。

互換性チェック

互換性チェックでは、チャネルのすべての物理ポートで同一のパラメータ設定が確実に使用されるようにします。そうでない場合、ポートがポートチャネルに所属できません。互換性チェックは、ポートをポートチャネルに追加する前に実施します。

互換性チェックでは、ポートチャネルの両側で次のパラメータと設定が一致していることを確認します。

- 機能パラメータ（インターフェイスのタイプ、両端のギガビット イーサネット、両端のファイバ チャネル）。
- 管理上の互換性パラメータ（速度、モード、レート モード、ポート VSAN、許可 VSAN リスト、およびポート セキュリティ）

（注） 共有レートモードのポートではポートチャネルやトランキングポートチャネルを形成できません。

- 動作パラメータ（リモート スイッチ WWN およびトランキング モード）

リモート スイッチの機能パラメータと管理パラメータおよびローカル スイッチの機能パラメータと管理パラメータに互換性がない場合、ポートは追加できません。互換性チェックが正常であれば、インターフェイスは正常に動作し、対応する互換性パラメータ設定がこれらのインターフェイスに適用されます。

中断および隔離ステート

動作パラメータに互換性がない場合、互換性チェックは失敗し、インターフェイスは設定されたモードに基づいて中断ステートまたは隔離ステートになります。

- インターフェイスは、ON モードに設定されている場合、一時停止状態になります。
- インターフェイスは、ACTIVE モードに設定されている場合、分離状態になります。

インターフェイスの強制追加

ポートチャネルにより、ポート設定の上書きを強制することができます。この場合、インターフェイスはポートチャネルに追加されます。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- ACTIVEモードを使用する場合、ポートチャネルポートは追加から自動的に回復します。

（注） インターフェイス内からポートチャネルを作成するときは、force オプションを使用できません。

メンバーの強制追加後、使用するモード（ACTIVE および ON）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

ポートチャネルからのインターフェイスの削除

物理インターフェイスをポートチャネルから削除すると、チャネルメンバーシップは自動的に更新されます。削除されたインターフェイスが最後の動作可能なインターフェイスである場合は、ポートチャネルのステータスは、ダウン状態に変更されます。ポートチャネルからインターフェイスを削除すると、ポートチャネルのチャネルサイズおよび帯域幅は減少します。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトのONモードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブモードを使用する場合、ポートチャネルポートは削除から自動的に回復します。

メンバーを削除すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します。

ポートチャネルプロトコル

Cisco SAN-OS の前バージョンでは、ポートチャネルで同期をサポートするために管理作業がさらに必要となっていました。Cisco NX-OS ソフトウェアには、強力なエラー検出機能および同期機能があります。チャネル グループを手動で設定できますが、自動的に作成することもできます。どちらの場合でも、チャネルグループの機能および設定可能なパラメータは同じです。対応付けられたポート チャネル インターフェイスに適用される設定の変更は、チャネル グループ内のすべてのメンバーに伝播されます。

ポートチャネル設定をやり取りするプロトコルは、すべてのCisco MDS スイッチで使用できます。この追加機能により、非互換ISLでのポートチャネル管理が簡単になります。追加された自動作成モードでは、互換性のあるパラメータを持つISLでチャネル グループを自動的に作成でき、手動での作業は必要ありません。

デフォルトではポートチャネルプロトコルがイネーブルになっています。

ポートチャネルプロトコルにより、Cisco MDS スイッチにおけるポートチャネル機能モデルが拡張されます。ポート チャネル プロトコルは、Exchange Peer Parameters（EPP）サービスを使用して、ISL のピア ポート間の通信を行います。各スイッチは、ピアポートから受信した情報、およびローカル設定と動作値を使用し、それがポートチャネルの一部であるかどうかを判断します。このプロトコルでは、一連のポートが確実に同一ポートチャネルの一部になります。すべてのポートが互換性のあるパートナーを持つ場合だけ、ポート一式が同一のポートチャネルに属せます。

ポートチャネルプロトコルでは、次の 2 つのプロトコルが使用されます。

- 起動プロトコル：自動的に誤設定を検出するため、これらを修正できます。このプロトコルでは両側でポートチャネルが同期されるので、特定フローのすべてのフレーム（送信元 FC ID、宛先 FC ID、OX_ID によって識別）は両方向で同一の物理リンクによって伝送されます。これにより、書き込みアクセラレーションのようなアプリケーションが、FCIP リンクでポートチャネル用に動作するようになります。
- 自動作成プロトコル：互換性があるポートがポートチャネルに自動的に集約されます。

ここでは、ポートチャネルプロトコルの設定方法について説明します。ここで説明する内容は、次のとおりです。

チャネルグループの作成

（注） HP c-Class BladeSystem 用シスコ ファブリック スイッチおよび IBM BladeSystem 用シスコ ファブリック スイッチの内部ポートでは、チャネル グループがサポートされません。

リンク A1-B1 が最初にアップすると仮定すると (図 1-9 を参照)、そのリンクは個別のリンクとして動作します。次のリンク（たとえばA2-B2）がアップすると、ポートチャネルプロトコルは、このリンクがリンク A1-B1 と互換性があるかどうかを識別し、それぞれのスイッチでチャネルグループ 10 および 20 を自動的に作成します。リンク A3-B3 がチャネル グループ（ポートチャネル）に参加できるということは、それぞれのポートに互換性の設定があるということです。リンク A4-B4 が個別リンクとして動作するということは、このチャネル グループのその他のメンバー ポートとの互換性が、2 つのエンド ポート設定にないということです。

チャネル グループ番号は動的に選択され、片側でチャネル グループを形成するポートの管理上の設定は、新しく作成されるチャネル グループに適用可能となります。動的に選択されるチャネルグループ番号は、スイッチでポートが初期化される順序に基づくので、同一セットのポートチャネルでも、リブートすると異なることがあります。

次の表に、ユーザー設定のチャネルグループと自動設定のチャネルグループの相違点を示します。

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
ユーザが手動で設定します。	2 つの互換性のあるスイッチ間で互換性のあるリンクがアップしたときに自動的に作成されます（両端のすべてのポートでチャネル グループの自動作成がイネーブルになっている場合）。
メンバ ポートはチャネル グループの自動作成には参加できません。自動作成機能は設定できません。	これらのポートは、ユーザ設定のチャネル グループのメンバにはなりません。
チャネルグループのポートのサブセットでポートチャネルを形成できます。互換性がないポートは、ON モード設定またはACTIVEモード設定により、一時停止状態か分離状態になります。	チャネルグループに組み込まれるすべてのポートがポートチャネルに参加します。メンバーポートが分離状態や一時停止状態になることはありません。リンクに互換性がない場合、そのメンバーポートはチャネルグループから削除されます。
ポートチャネルで行った管理上の設定はチャネルグループのすべてのポートに適用され、ポート チャネル インターフェイスの設定は保存できます。	ポートチャネルで行った管理上の設定はチャネルグループのすべてのポートに適用されますが、メンバーポートの設定は保存され、ポート チャネル インターフェイスの設定は保存されません。このチャネル グループは、必要に応じて明示的に変更できます。

ユーザ設定のチャネル グループ	自動設定のチャネル グループ
任意のチャネル グループの削除およびチャネル グループへのメンバの追加が可能です。	チャネル グループは削除できません、メンバーの追加や削除もできません。メンバ ポートが存在しない場合、チャネル グループは削除されます。

自動作成

自動作成プロトコルには次の機能があります。

- 自動作成機能をイネーブルにした場合、ポートはポートチャネルの一部として設定できません。これらの 2 つの設定を同時に使用できません。
- 自動作成は、ポートチャネルをネゴシエーションするため、ローカルポートとピアポートの両方でイネーブルにする必要があります。
- 集約は、次の 2 通りの方法で実行されます。
  - 互換性のある自動作成ポートチャネルにポートが集約されます。
  - 互換性がある別のポートにポートが集約され、新しいポートチャネルが形成されます。
- 新しく作成されたポートチャネルは、可用性に基づいて大きいものから順に最大のポートチャネル（第 1 世代スイッチまたは第 1 世代スイッチと第 2 世代スイッチの組み合わせの場合は 128、第 2 世代スイッチの場合は 256）から割り当てられます。128 または 256 の番号すべてが使用されている場合、集約は行われません。
- メンバーシップの変更または自動作成されたポートチャネルの削除はできません。
- 自動作成を無効化すると、すべてのメンバー ポートは自動作成ポートチャネルから削除されます。
- 最後のメンバーが自動作成ポートチャネルから削除されると、チャネルは自動的に削除され、番号は解放されて再利用されます。
- 自動作成ポートチャネルは、リブート後に維持されません。自動作成されたポートチャネルは、手動で設定することにより、永続的なポートチャネルと同じように表示させることができます。ポートチャネルを持続させた場合、自動作成機能はすべてのメンバーポートでディセーブルになります。
- 自動作成機能は、ポート単位またはスイッチ内のすべてのポートに対して、イネーブルまたはディセーブルに設定できます。この設定がイネーブルの場合、チャネル グループ モードはアクティブと見なされます。このタスクのデフォルトはディセーブルです。
- インターフェイスに対してチャネル グループの自動作成がイネーブルになっている場合、最初に自動作成をディセーブルにしてから、以前のソフトウェア バージョンにダウングレードするか、または手動設定されたチャネル グループでインターフェイスを設定する必要があります。

（注） Cisco MDS 9000 ファミリの任意のスイッチで自動作成をイネーブルにする場合は、スイッチ間の最低 1 つの相互接続ポートで自動作成を設定しないことを推奨します。2 つのスイッチ間のすべてのポートを自動作成機能で同時に設定すると、自動作成ポートチャネルにポートが追加されるとき、ポートが自動的にディセーブルになって再度イネーブルになるので、この 2 つのスイッチ間でトラフィックが混乱することがあります。

手動設定チャネルグループ

ユーザによって設定されたチャネル グループを自動作成チャネル グループに変更できません。ただし、自動作成されたチャネル グループから手動チャネル グループへの変更は可能です。このタスクは、実行すると元に戻すことはできません。チャネル グループ番号は変化しませんが、メンバー ポートは手動設定チャネル グループのプロパティに従って動作し、チャネル グループの自動作成はすべてのメンバー ポートで暗黙的にディセーブルになります。

ヒント 持続をイネーブルにする場合は、ポートチャネルの両側でイネーブルにしてください。

ポートチャネルの設定の前提条件

ポートチャネルを設定する前に、次の注意事項を守ってください。

- スイッチングモジュール間でポートチャネルを設定し、スイッチングモジュールのリブートまたはアップグレードの際の冗長性を実装してください。
- 1 つのポートチャネルをさまざまなセットのスイッチに接続しないでください。ポートチャネルでは、同一セットのスイッチ間におけるポイントツーポイント接続が必要です。

第 1 世代スイッチングモジュールを含むか、第 1 世代および第 2 世代のスイッチング モジュールを含むスイッチでは、最大で 128 のポートチャネルを設定できます。第 2 世代スイッチングモジュールを含むか、第 2 世代および第 3 世代のスイッチング モジュールを含むスイッチでは、最大で 256 のポートチャネルを設定できます。

ポートチャネルの設定を誤った場合は、誤設定メッセージを受信することがあります。このメッセージを受信した場合、エラーが検出されたため、ポートチャネルの物理リンクはディセーブルになります。

ポートチャネルのエラーは、次の要件を満たしていない場合に検出されます。

- ポートチャネルの両端のスイッチが、同じ数のインターフェイスに接続されている必要があります。
- 各インターフェイスは、対応する反対側のインターフェイスに接続される必要があります（無効な設定例については、図 1-11 を参照してください）。
- ポートチャネルの設定後に、ポートチャネルのリンクは変更できません。ポートチャネルの設定後にリンクを変更する場合は、ポートチャネル内のインターフェイスにリンクを再接続してリンクを再びイネーブルにします。

3 つすべての条件が満たされていない場合、そのリンクはディセーブルになっています。

そのインターフェイスに show interface コマンドを入力して、ポートチャネルが設定どおりに機能していることを確認します。

ポートチャネルの設定に関するガイドラインと制約事項

この項では、この機能のガイドラインと制限事項について説明します。

Cisco MDS 9000 シリーズスイッチの一般的なガイドライン

Cisco MDS 9000 ファミリスイッチは、スイッチごとに次の数のポートチャネルをサポートします。

- 第 1 世代のスイッチングモジュールのみを含むスイッチは、F ポートチャネルおよび TF ポートチャネルをサポートしません。
- 第 1 世代スイッチングモジュールを含むか、第 1 世代および第 2 世代のスイッチングモジュールを含むスイッチでは、最大で 128 のポートチャネルがサポートされます。第 2 世代のポートのみをポートチャネルに組み込むことができます。
- 第 2 世代のスイッチングモジュールを含むか、第 2 世代および第 3 世代のスイッチングモジュールを含むスイッチでは、ポートチャネルごとに最大で 16 インターフェイスで 256 のポートチャネルがサポートされます。
- ポートチャネル番号は、各チャネルグループの一意の識別番号です。この番号の範囲は 1 ～ 256 です。

第 1 世代ポートチャネルの制限事項

ここでは、次の第 1 世代ハードウェアのポートチャネルにポートチャネルメンバーを作成および追加する場合の制約事項について説明します。

- 32 ポートの 2 Gbps または 1 Gbps スイッチングモジュール
- MDS 9140 および 9120 スイッチ。

第 1 世代ハードウェアのホスト最適化ポートを設定する場合は、ポートチャネルに関する次の注意事項が適用されます。

- 32 ポート スイッチングモジュールで write erase コマンドを実行し、no system default switchport shutdown コマンドを含むテキストファイルからスイッチに保存済み設定をコピーする場合、手動設定せずに E ポートをアップさせるには、テキストファイルをスイッチに再度コピーする必要があります。
- Cisco MDS 9100 シリーズの任意の（またはすべての）フル回線レートポートをポートチャネルに組み込むことができます。
- Cisco MDS 9100 シリーズのホスト最適化ポートは、32 ポート スイッチング モジュールと同じポートチャネルのルールに従います。各 4 ポートグループの最初のポートだけがポートチャネルに組み込まれます。

- 各 4 ポートのグループの最初のポートだけを E ポートとして設定できます（ポート 1 ～ 4 の最初のポート、ポート 5 ～ 8 の 5 のポートなど）。そのグループの最初のポートがポートチャネルとして設定された場合は、各グループのその他3つのポート（ポート 2 ～ 4、6 ～ 8 など）は使用できず、シャットダウンステートのままになります。
- その他 3 つのポートのいずれかがシャットダウンステート以外で設定されている場合は、最初のポートをポートチャネルとして設定できません。その他 3 つのポートは、引き続きシャットダウン ステート以外になります。

F および TF ポートチャネルの制限事項

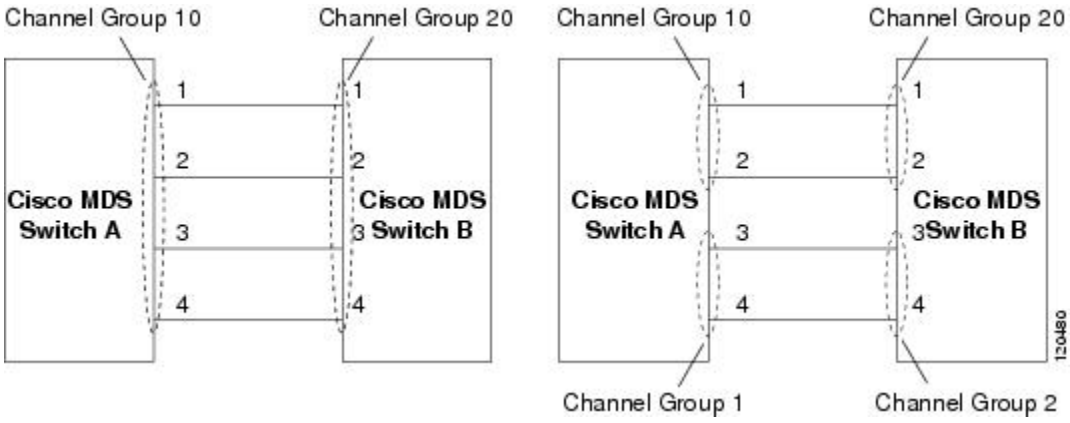
F ポートチャネルおよび TF ポートチャネルには、次の注意事項と制約事項が適用されます。

- ポートを F モードとしておく必要があります。
- 自動作成はサポートされません。
- 複数の FCIP インターフェイスを WA でグループ化する場合は、ポートチャネル インターフェイスが ACTIVE モードである必要があります。
- ON モードはサポートされません。サポートされるのは ACTIVE-ACTIVE モードだけです。デフォルトでは、NPV スイッチのモードは ACTIVE です。
- MDS スイッチの F ポートチャネル経由でログインしたデバイスは、IVR の非 NAT 設定でサポートされません。このデバイスをサポートするのは IVR NAT 設定だけです。
- ポートセキュリティルールは、物理 pWWN だけで単一リンクレベルで実行されます。
- FC-SP では、ポートチャネルのメンバーごとに最初の物理 FLOGI だけを認証します。
- FLOGI ペイロードは VF ビットだけを伝送して FLOGI 交換後にプロトコルの使用をトリガーするため、このビットは上書きされます。NPV スイッチの場合は、コアに Cisco WWN が設定されているので PCP プロトコルの開始を試行します。
- F ポートチャネル経由でログインする N ポートのネームサーバー登録では、ポート チャネル インターフェイスの fWWN を使用します。
- DPVM 設定はサポートされません。
- ポートチャネルのポート VSAN は DPVM を使用して設定できません。
- Dynamic Port VSAN Management（DPVM）データベースの問い合わせは各メンバーの最初の物理 FLOGI についてだけ行われるため、ポート VSAN は自動的に設定されます。
- DPVM では FC_ID を VSAN にバインドしませんが、pWWN を VSAN にバインドします。問い合わせが行われるのは物理 FLOGI についてだけです。

有効なポートチャネルと無効なポートチャネルの例

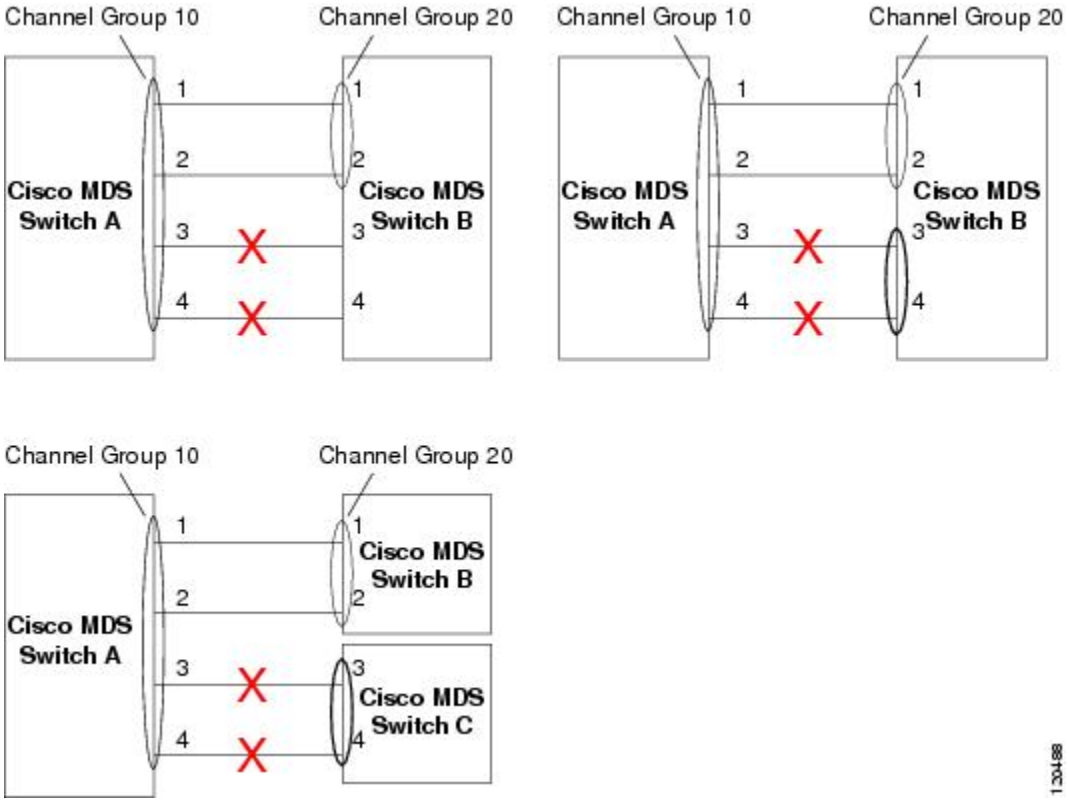
ポートチャネルは、デフォルト値で作成されます。その他の物理インターフェイスと同じように、このデフォルト設定を変更できます。次の図は、有効なポートチャネルの設定例を示しています。

図 *6:* 有効なポートチャネルの設定



次の図は、有効な設定例を示しています。リンクが1、2、3、4の順番でアップした場合、ファブリックの設定が誤っているため、リンク 3 および 4 は動作上ダウンします。

図 *7:* 誤った設定



デフォルト設定

次の表に、ポートチャネルのデフォルト設定を示します。

表 *6 :* デフォルト *SAN* ポートチャネルパラメータ

パラメータ	デフォルト
ポート チャネル	FSPF はデフォルトでイネーブルになっています。
ポート チャネルの作成	管理上のアップ状態
デフォルト ポート チャネル モード	ON モード（非 NPV スイッチおよび NPIV コア スイッチ）。 ACTIVE モード（NPV スイッチ）
自動作成	ディセーブル

[Create Port Channel] ウィザード

Nexusダッシュボード ファブリック コントローラ Web UI で新しいポートチャネルの作成ウィザードを使用してポートチャネルを作成するには、次の手順を実行します。

手順

ステップ 1 **[新しいポートチャネルの作成（Create a new Port Channel）]** を [アクション（Actions）] ドロップダウンリストから選択します。

[新しいポートチャネルの作成（Create New Port Channel）] をクリックして、ポートチャネルの作成ウィザードを起動します。

ステップ 2 [スイッチペアの選択（Select Switch Pair）] 画面で、次の手順を実行します。

a) [ファブリック（Fabric）] ドロップダウンから適切なファブリックを選択します。

このリストには、ポートチャネルにまだ存在しない、間に ISL があるファブリック内のスイッチペアが含まれています。

b) FC ポートチャネルでリンクするスイッチペアを選択します。

NPIV コアと NPV スイッチの間に NPV リンクがある場合、スイッチペアと NPV リンクの数を表示するには、NPIV スイッチで **feature fport-channel-trunk** コマンドを使用して F ポートトランキングとチャネリングプロトコルを有効にする必要があります

c) [次へ（Next）] をクリックします。

ステップ 3 [ISL の選択（Select ISLs）] 画面で、1 つ以上の ISL またはリンクを選択して、スイッチペア間に新しいチャネルを作成します。

a) [利用可能（Available）] エリアの ISL のリストから、右矢印を選択してクリックし、ISL を [選択済み（Selected）] エリアに移動します。

b) [次へ（Next）] をクリックします。

ステップ 4 **[チャネルの設定（Configure Channel）]** 画面で、チャネル属性を定義または編集します。

a) [チャネル ID（Channel ID）] フィールドには、次の未使用のチャネル ID が入力されます。必要に応じて、各スイッチのチャネル ID または説明を変更します。

チャネル ID の範囲は 1 ～ 256 です。

b) FICON ポート アドレスは、スイッチで FICON が有効になっている場合にのみ有効です。ドロップダウンリストから、スイッチの適切な FICON ポートアドレスを選択します。ポートチャネルポートに割り当てるポートアドレスを選択します。

c) [Channel Attributes（チャネル属性）] エリアで、速度を設定するには、適切なオプションボタンをクリックします。

d) 適切な [トランクモード（Trunk Mode）] オプションボタンを選択して、ポートチャネルのリンクでトランキングを有効にします。

- TE ポート間にリンクが存在する場合は、**[トランク（trunk）]** を選択します。
- E ポート間にリンクが存在する場合は、**[nonTrunk]** を選択します。
- 不明な場合は、**[自動（auto）]** を選択します。

e) [ポート VSAN（Port VSAN）] フィールドに、トランキングが有効になっていない場合に使用する必要があるポート VSAN のインターフェイス ID を入力します。

トランキングが有効になっている場合でも、すべてのインターフェイスにはポート VSAN が必要です。トランキングが有効になっている場合、このポート VSAN は使用されません。ただし、トランキングが無効になっている場合に、ネットワークがデフォルトで使用する VSAN を認識できるように、スイッチはポートを設定する必要があります。

f) VSAN リストフィールドには、ポートチャネルがトランキングに使用できるようにする VSAN のリストが表示されます。

トランクモードが **[nonTrunk]** または **[自動（auto）]** に設定されている場合、このフィールドは無効になります。

g) [コアスイッチ帯域幅（Core Switch Bandwidth）] フィールドで、専用または共有オプションボタンを選択して、スイッチの帯域幅を割り当てます。

この帯域幅は、NPIV スイッチと NPV スイッチ間のポートチャネルにのみ適用されます。

h) **[管理の強制（Force Admin）]**、**[トランク（Trunk）]**、**[速度（Speed）]**、および **[VSAN 属性を一致させる（VSAN attributes to be identical）]** チェックボックスをオンにして、チャネルのすべての物理ポートで同じパラメータ設定が使用されるようにします。これらの設定が同じでない場合、ポートはポートチャネルに属することができません。

ステップ 5 **[前へ（Previous）]** をクリックして前の画面に戻り、設定を編集します。**[新しいポートチャネルの作成（Create New Port Channel）]** をクリックして、ポートチャネルを設定します。

処理が正常に完了したことを知らせるメッセージが表示されます。

既知のポートチャネルの編集

Nexusダッシュボード ファブリック コントローラ Web UI でポートチャネルの編集ウィザードを使用してポートチャネルを編集するには、次の手順を実行します。

手順

ステップ 1 **[ポートチャネルの編集（Edit Port Channel）]** を **[アクション（Actions）]** ドロップダウンリストから選択します。

[ポートチャネルの編集（Edit Port Channel）] をクリックして、ポートチャネルの作成ウィザードを起動します。

ステップ 2 [スイッチペアの選択（Select Switch Pair）] 画面で、次の作業を実行します。

a) [ファブリック（Fabric）] ドロップダウンリストから適切なファブリックを選択します。

間にポートチャネルがあるスイッチペアは、以下のエリアにリストされています。

b) ポートチャネルを編集するスイッチペアを選択します。

c) [次へ（Next）] をクリックします。

ステップ 3 [ポートチャネルの選択（Select Port Channel）] 画面で、編集するポートチャネルを選択します。

[次へ（Next）] をクリックします。

ステップ 4 [ポートチャネルの編集（Edit Port Channel）] 画面で、目的の ISL を選択します。

a) 左右の矢印をクリックして、使用可能な ISL を選択します。

（注） 変更を保存すると、選択した ISL がポートチャネルに含まれます。選択した ISL リストが空の場合、[ポートチャネルの削除が空です（Delete Port Channel is Empty）] チェックボックスが有効になります。

b) ISL を選択しない場合は、**[ポートチャネルが空の場合、削除する（Delete Port Channel If Empty）]** チェックボックスをオンにして、ポートチャネルを削除します。

c) **[管理の強制（Force admin）]**、**[トランク（Trunk）]**、**[速度（speed）]**、**[VSAN 属性を同一にする（VSAN attributes to be identical）]** チェックボックスをオンにして、管理、トランク、速度、および VSAN 属性に同一の値を選択します。

d) [次へ（Next）] をクリックします。

ステップ 5 **[ポートチャネルの保存（Save port channel）]** をクリックして変更を適用します。

NPV Links

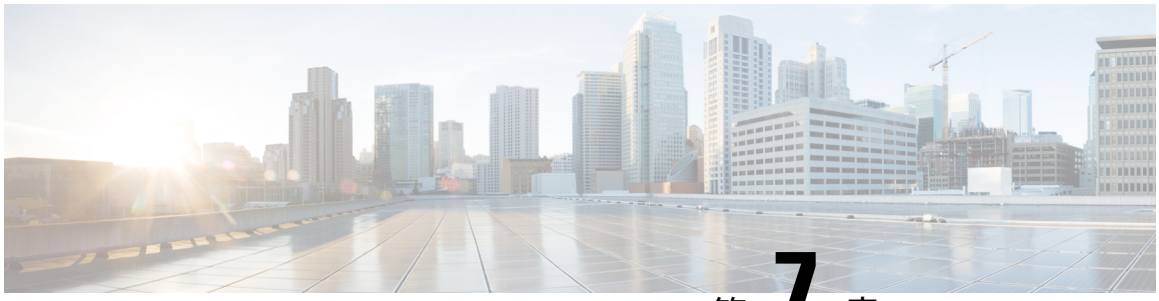
NPV リンクウィンドウが表示されます。この表は、SAN ファブリック上の NPV リンクのパフォーマンスを示しています。ドロップダウンを使用して、24時間、週、月、および年でビューをフィルタ処理できます。

ドロップダウンを使用して、**24 時間、週、月**、および**年**でビューをフィルタ処理できます。

[名前（Name）]列の [チャート（chart）] アイコンをクリックし、過去 24 時間のトラフィックのリストを表示します。

他にもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行して NPV リンクの詳細情報を表示することもできます。

- この情報の時間範囲を変更するには、右上の隅のドロップダウンリストから選択します。
- 期間を指定して詳細情報を表示するには、スライダコントロールをドラッグして、表示する期間を指定します。
- チャートアイコンを使用して、さまざまなビューでトラフィックチャートを表示します。アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[補間（Interpolate）]** することもできます。
- スプレッドシートにデータをエクスポートするには、右上の隅の**[エクスポート（Export）]** アイコンをクリックしてから **[保存（Save）]** をクリックします。
- リアルタイム情報を表示するには、**[チャート（Chart）]** メニューの **[リアルタイム（Real Time）]** を選択します。



第 7 章

インターフェイス

インターフェイス

このセクションでは、FC ポート、イーサネットポート、ポートグループなどの SAN インターフェイスに関する情報を提供します。

FC ポート

[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] を選択して、FC ポートに関する情報を表示します。

FC ポートのインベントリ情報の表示

[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [インベントリ（Inventory）] タブを選択して、ファイバチャネルインターフェイスのリストを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [インベントリ（Inventory）]** に表示されるフィールドについて説明します。

フィールド	説明
Status	インターフェイスのステータスを指定します。
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。
エンクロージャ	エンクロージャを指定します。

フィールド	説明
デバイス名（Device Name）	デバイス名を指定します。
VSAN	インターフェイスが属する VSAN を指定します。
スイッチインターフェイス	インターフェイス名を指定します。
Type	インターフェイス タイプを指定します。
ポートWWN	ポートのワールドワイド名（pWWN）を指定します。
スピード	インターフェイスの速度を指定します。
FCID	インターフェイス FCID を指定します。

FC ポートのパフォーマンス情報の表示

[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [パフォーマンス（Performance）] タブを選択して、ファイバ チャネル インターフェイスのパフォーマンスを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [パフォーマンス（Performance）]** に表示されるフィールドについて説明します。**[最終日を表示（Show last day）]** ドロップダウンリストから **[日、週、月（Day, Week, Month）]**、および **[年（Year）]** オプションを使用して、データをフィルタ処理できます。**[ホストポートの表示（Show Host Ports）]** ドロップダウンリストを使用して、**[ホストポート（Host Ports）]** と **[ストレージポート（Strage Ports）]** をフィルタ処理することもできます。

パフォーマンスを有効にするには、**[ファブリック（Fabric）]** ウィンドウに移動し、必要なファブリックを選択して、**[アクション（Actions）] > [パフォーマンスの設定（Configure Performance）]** を選択します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。

フィールド	説明
名前	インターフェイス名を指定します。**[名前（Name）]** 列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および**[年（Year）]**オプションを使用してデータをフィルタ処理できます。
VSAN	インターフェイスが属する VSAN を指定します。
スイッチインターフェイス	インターフェイス名を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

FC FICON ポートの表示

[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [FICON] タブを選択して、ファイバチャネル FICON インターフェイスのリストを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [FC ポート（FC Ports）] > [FICON]** に表示されるフィールドについて説明します。**[最終日の表示（Show last day）]** メニュー ドロップダウンリストを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。
スイッチインターフェイス	スイッチインターフェイスを指定します。
説明	インターフェイスの説明を指定します。
FCID	関連するインターフェイス FCID を指定します。
モード（Mode）	インターフェイス モードを指定します。
FICON ID	FICON ID を指定します。
接続先	インターフェイスの接続先を指定します。
VSAN	インターフェイスが属する VSAN を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	

フィールド	説明
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

イーサネットポートに関するパフォーマンス情報の表示

[SAN] > [インターフェイス（Interfaces）] > [イーサネット（Ethernet）] タブを選択して、イーサネット インターフェイスのリストを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [イーサネット（Ethernet）]** に表示されるフィールドについて説明します。**[最終日の表示（Show last day）]** メニュー ドロップダウンリストを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。
名前	インターフェイス名を指定します。**[名前（Name）]** 列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および**[年（Year）]** オプションを使用してデータをフィルタ処理できます。
説明	インターフェイスの説明を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。

フィールド	説明
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

ポートグループに関するパフォーマンス情報の表示

[SAN] > [インターフェイス（Interfaces）] > [ポートグループ（Port Groups）] タブを選択して、ポートグループのリストを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [ポートグループ（Port Groups）]** に表示されるフィールドについて説明します。**[過去 24 時間の表示（Show last 24 hours）]** メニューのドロップダウンリストを使用して、**24 時間**、**週**、**月**、および**年**でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。

フィールド	説明
ポート グループ名	ポートグループ名を指定します。名前をクリックすると、ポートグループのメンバーが表示されます。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

ポートグループメンバー

[SAN] > [インターフェイス（Interfaces）] > [ポートグループ（Port Groups）] を選択し、ポートグループ名をクリックして、ポートグループのメンバーを表示します。

次の表では、**[ポートグループメンバー（Port Group Member）]** に表示されるフィールドについて説明します。

フィールド	説明
ポートグループメンバー	ポートグループメンバーを指定します。チャートアイコンをクリックして、選択したタイムラインに基づくポートグループメンバーのトラフィックのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および **[年（Year）]** オプションを使用してデータをフィルタ処理できます。
スピード	ポートグループメンバーを指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。

フィールド	説明
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

オプティクスのパフォーマンス情報の表示

[SAN] > [インターフェイス（Interfaces）] > [オプティクス（Optics）] タブを選択して、光ファイバのリストを表示します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [オプティクス（Optics）]** に表示されるフィールドについて説明します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。
スイッチ	スイッチ名を指定します。
インターフェイス	インターフェイス名を指定します。**[インターフェイス（Interfaces）]** 列のチャートアイコンをクリックして、選択したタイムラインに従って、そのデバイスの光学パラメータのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および **[年（Year）]** オプションを使用してデータをフィルタ処理できます。
温度（C）	平均、最低、最高温度を指定します。
電流（mA）	各パラメータの平均値を指定します。

フィールド	説明
OPRxPower	平均、最小、および最大の光受信出力を指定します。
OPTxPower	平均、最小、および最大の光送信出力を指定します。
Voltage	平均、最小、および最大電圧を指定します。

Cisco Web Nexusダッシュボード ファブリック コントローラ UI からすべての FC ポートに接続されているデバイスの光メトリック情報を表示するには、次の手順を実行します。

1. **[SAN] > [インターフェイス（Interfaces）] > [オプティクス（Optics）]** を選択します。

   [オプティクス（Optics）] ウィンドウが表示されます。

2. **[属性でフィルタ（Filter by attributes）]** フィールドを使用してテーブルを並べ替えると、**ファブリック**、**スイッチ**、**インターフェイス**、**温度**、**電流**、**電力**、および**電圧**によるフィルタ処理を有効にすることができます。

3. **[最終日の表示（Show last day）]** ドロップダウンを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理できます。

4. ファブリック名をクリックすると、ページの右側にファブリックの正常性ステータスが表示されます。

5. ファブリックウィンドウの **[起動（Launch）]** アイコンをクリックして、ファブリックの概要ページに移動します。

カスタムポートグループ

[SAN] > [インターフェイス（Interfaces）] > [カスタムポートグループ（Custom Port Groups）] タブを選択して、カスタムポートグループを表示および作成します。

次の表では、**[SAN] > [インターフェイス（Interfaces）] > [カスタムポートグループ（Custom Port Groups）]** に表示されるフィールドについて説明します。

フィールド	説明
グループ名 （Group Name）	ポートグループ名を指定します。名前をクリックしてパフォーマンスを表示し、ポートグループを設定します。詳細については、カスタムポートグループのパフォーマンスの表示 （118 ページ）およびカスタムポートグループの設定 （119 ページ）を参照してください。
デバイス	デバイスの番号を指定します。
インターフェイス	インターフェイスの番号を指定します。

次の表で、**[SAN]>[インターフェイス（Interfaces）]>[カスタムポートグループ（Custom Port Group）]** で表示される **[アクション（Actions）]** メニュー ドロップダウン リストの アクション項目について説明します。

アクション項目	説明
ポートグループの作成	テーブルからポートグループを選択し、**[ポートグループの作成（Create Port Group）]** を選択してポートグループ名を指定し、**[保存して終了（Save & Exit）]** をクリックしてカスタムポートグループを作成します。
ポートグループの編集	テーブルからポート グループを選択し、**[ポートグループの編集（Edit port group）]** を選択してポート グループを編集します。
Delete	テーブルからポートグループを選択し、**[削除（Delete）]** を選択してポートグループを削除します。

カスタムポートグループのパフォーマンスの表示

[SAN]>[インターフェイス（Interfaces）]>[カスタムポートグループ（Custom Port Groups）] を選択し、ポートグループ名をクリックして、ポートグループのパフォーマンスを表示します。

次の表では、カスタムポートの **[パフォーマンス（Performance）]** タブに表示されるフィールドについて説明します。

フィールド	説明
デバイス	デバイス名を指定します。
接続先	インターフェイスの接続先を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
平均	着信エラーまたは破棄の平均を指定しました。

フィールド	説明
ピーク	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

[最終日の表示（Show last day）] メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

カスタムポートグループの設定

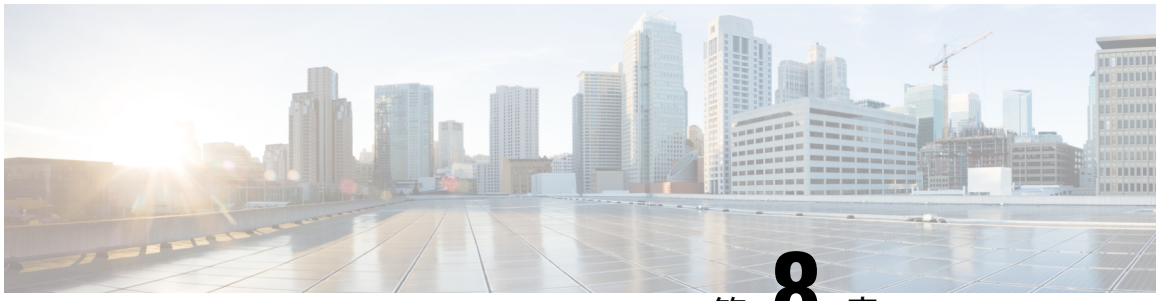
[SAN] > [インターフェイス（Interfaces）] > [カスタムポートグループ（Custom Port Groups）] を選択し、ポートグループ名をクリックして、**[設定（Configuration）]** タブをクリックして、カスタムポートグループを設定します。

次の表では、カスタムポートの **[設定（Configuration）]** タブに表示されるフィールドについて説明します。

フィールド	説明
デバイス	デバイス名を指定します。デバイス名をクリックすると、ページの右側にデバイスの状態が表示されます。
接続先	インターフェイスの接続先を指定します。
説明	インターフェイスの説明を指定します。

次の表では、**[設定（Configuration）]** タブに表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
Add Interfaces	**[インターフェイスを追加する（Add Interfaces）]** を選択してポートグループにインターフェイスを追加します。[インターフェイスを追加する（Add Interfaces）] ウィンドウでデバイスを選択し、**[次の手順 - インターフェイスを追加する（Next Step - Add Interfaces）]** をクリックします。ポートグループに追加するインターフェイスを選択して、**[保存して終了（Save & Exit）]** をクリックします。
Delete	テーブルからポートグループを選択し、**[削除（Delete）]** を選択してポートグループを削除します。



第 8 章

エンド デバイス

デバイス

[SAN] > [エンドデバイス（End Devices）] > [デバイス（Devices）] タブを選択して、ホストおよびストレージデバイスのリストを表示します。

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [デバイス（Devices）]** に表示されるフィールドについて説明します。**[最終日の表示（Show last day）]** メニュー ドロップダウンリストを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理します。**[ホストポートの表示（Show Host Ports）]** メニューのドロップダウンリストを使用して、**ホストポート** と **ストレージポート**でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある **[起動（Launch）]** アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要（Fabric Overview）] ウィンドウの詳細については、「ファブリックの概要 （56 ページ）」を参照してください。
エンクロージャ名	エンクロージャ名を指定します。

フィールド	説明
デバイス エイリアス	デバイスエイリアスを指定します。**[デバイスエイリアス（Device Alias）]** 列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および **[年（Year）]** オプションを使用してデータをフィルタ処理できます。
FCID	関連する FCID を指定します。
スイッチインターフェイス	スイッチインターフェイスを指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

ラック

[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] タブを選択して、ホストとストレージエンクロージャを表示します。

Cisco Nexusダッシュボード ファブリック コントローラ は、ファブリックの可視性をサーバーまで拡張し、ネットワークに接続されているエンドデバイス、SANストレージエンクロージャ、およびストレージシステムを検出および検索できるようにします。

エンクロージャの詳細を表示するには、表内のエンクロージャ名をクリックします。

このセクションは、次のトピックで構成されています。

インベントリエンクロージャ

[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [インベントリ（Inventory）] > [ホストエンクロージャ（Host Enclosures）] タブを選択して、ホストおよびストレージ インベントリ エンクロージャを表示します。

このセクションは、次のトピックで構成されています。

インベントリ ホスト エンクロージャ

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [インベントリ（Inventory）] > [ホストエンクロージャ（Host Enclosures）]** に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ	エンクロージャ名を指定します。詳細については、エンクロージャ名をクリックしてください。
OS	OS の詳細を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
WWN	World Wide Name（WWN）の数を指定します。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[SAN]>[エンドデバイス（End Devices）]>[エンクロージャ（Enclosures）]>[インベントリ（Inventory）]>[ホストエンクロージャ（Host Enclosures）]** に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルからエンクロージャを選択し、**[編集（Edit）]** を選択してエンクロージャ情報を更新します。
ストレージエンクロージャに変更	テーブルからエンクロージャを選択し、**[ストレージ エンクロージャに変更（Change to Storage Enclosure）]** を選択して、選択したエンクロージャをストレージ エンクロージャに変更します。

インベントリ ストレージ エンクロージャ

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [インベントリ（Inventory）] > [ストレージエンクロージャ（Storage Enclosures）]** に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ	エンクロージャ名を指定します。詳細については、エンクロージャ名をクリックしてください。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
WWN	World Wide Name（WWN）の数を指定します。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [インベントリ（Inventory）] > [ストレージエンクロージャ（Storage Enclosures）]** に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルからエンクロージャを選択し、**[編集（Edit）]** を選択してエンクロージャ情報を更新します。
ホストエンクロージャに変更	テーブルからエンクロージャを選択し、**[ホストエンクロージャに変更（Change to Host Enclosure）]** を選択して、選択したエンクロージャをホストエンクロージャに変更します。

パフォーマンスエンクロージャ

[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [パフォーマンス（Performance ）] > [ホストエンクロージャ（Host Enclosures）] タブを選択して、ホストおよびストレージ パフォーマンス エンクロージャを表示します。

このセクションは、次のトピックで構成されています。

パフォーマンス ホスト エンクロージャ

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures ）] > [パフォーマンス（Performance ）] > [ホストエンクロージャ（Host Enclosures）]** に表示されるフィールドについて説明します。**[最終日の表示（Show last day）]** メニュー ドロップダウンリストを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理します。

フィールド	説明
エンクロージャ名	エンクロージャ名を指定します。エンクロージャ名をクリックして、詳細を表示します。チャートアイコンをクリックして、選択したタイムラインに基づくそのデバイスのトラフィックのグラフを表示します。**[日（Day）]**、**[週（Week）]**、**[月（Month）]**、および **[年（Year）]** オプションを使用してデータをフィルタ処理できます。
受信/送信/エラー/破棄	
平均	受信、送信、エラーまたは破棄の平均速度を指定します。
ピーク	受信、送信、エラーまたは破棄のピーク使用率を指定します。
Rx + Tx	受信速度と送信速度の合計を指定します。
最終更新日	最後に更新された日時を示します。

パフォーマンス ストレージ エンクロージャ

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures）] > [インベントリ（Inventory）] > [ストレージエンクロージャ（Storage Enclosures）]** に表示されるフィールドについて説明します。

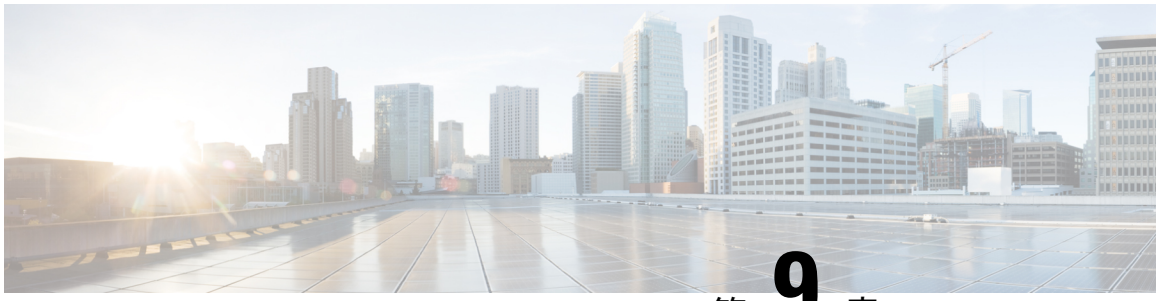
フィールド	説明
エンクロージャ名	エンクロージャ名を指定します。
受信/送信/エラー/破棄	
平均	受信、送信、エラーまたは破棄の平均速度を指定します。
ピーク	受信、送信、エラーまたは破棄のピーク使用率を指定します。
最終更新日	最後に更新された日時を示します。

[最終日の表示（Show last day）] メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

エンクロージャメンバー

次の表では、**[SAN] > [エンドデバイス（End Devices）] > [エンクロージャ（Enclosures ）] > [パフォーマンス（Performance）]** に表示されるフィールドについて説明します。エンクロージャメンバーは、ホストおよびストレージのパフォーマンスエンクロージャについて表示できます。**[最終日の表示（Show last day）]** メニュー ドロップダウンリストを使用して、**日**、**週**、**月**、および**年**でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。名前をクリックすると、ページの右側にファブリックの状態に関する情報が表示されます。
Device	デバイス名を指定します。
スピード	デバイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
エラー/破棄	
平均	平均エラーまたは破棄速度を指定します。
ピーク	エラーまたは破棄速度のピーク使用率を指定します。
最終更新日	最後に更新された日時を示します。



第 9 章

低速ドレイン分析

分析

分析では、スイッチレベルおよびポートレベルで低速ドレインの統計を表示できます。任意の期間内で低速ドレインの問題をモニタリングできます。データをチャート形式で表示し、分析のためにデータをエクスポートできます。また、txwait、ドロップ、クレジット損失回復、使用率の超過、およびポートモニタイベントの高レベルビューを提供するトポロジを表示することもできます。

統計はキャッシュメモリに保存されます。したがって、サーバーが再起動されるか、新しい診断リクエストが発行されると、統計は失われます。

Note ログオフした後でも、ジョブはバックグラウンドで実行されます。

Procedure

ステップ 1 **[ファブリック（Fabric）]** ドロップダウンリストからファブリック名を選択します。

ステップ 2 **[期間（Duration）]** ドロップダウンリストから、スケジュールされたジョブに対して **[1 回（Once）]** または **[毎日（Daily）]** を選択します。**[1 回（Once）]** は、10 分、30 分、1 時間、カスタム時間などの間隔を含み、ジョブをすぐに実行します。**[毎日（Daily）]** では、開始時刻を選択し、選択した間隔でジョブを実行できます。オプションボタンを使用して、データを収集する間隔を選択します。

ステップ 3 **[分析の開始（Start Analysis）]** をクリックして、ポーリングを開始します。

サーバーは、ユーザーが定義した範囲に基づいて低速ドレインの統計を収集します。**[残り時間（Time Remaining）]** はページの右側に表示されます。

ステップ 4 **[分析の停止（Stop Analysis）]** をクリックして、ポーリングを停止します。

サーバーは、新しい診断リクエストが行われるまで、カウンタをキャッシュに保持します。時間切れになる前にポーリングを停止できます。

ステップ 5 各ファブリックの **[ファブリック（Fabric）]**、**[ポーリングのステータス（Status of polling）]**、**[開始（Start）]**、**[終了（End）]**、および **[期間（Duration）]** 列が表示されます。

ステップ 6 ファブリックを選択し、**[すべて削除（Delete All）]** または **[停止（Stop）]** をクリックして、ジョブを削除または停止します。

ファブリック名をクリックすると、ファブリックの詳細ビューが表示され、ファブリックのの詳細が表示されます。詳細については、「可視化, on page 128」を参照してください。

ステップ 7 **[デバイスインターフェイス（Device Interfaces）]** テーブルの **[スイッチ名（Switch Name）]** 列でスイッチ名をクリックして、スイッチの状態を表示します。

ステップ 8 **[デバイスインターフェイス（Device Interfaces）]** テーブルの **[インターフェイス（Interface）]** 列でインターフェイス名をクリックして、スイッチポートの低速ドレイン値をチャート形式で表示します。

[属性別フィルタ処理（Filter by attributes）] オプションを使用して、各列に定義された値に基づいて詳細を表示します。

[データのある行のみ（Only Rows With Data）] オプションを選択して、統計内のゼロ以外のエントリをフィルタ処理して表示します。

可視化

ファブリック名をクリックすると、選択したファブリックのトポロジが表示され、ファブリックのの詳細が表示されます。トポロジウィンドウには、さまざまなネットワーク要素に対応するノードとリンクが色分けされて表示されます。各要素について、カーソルを合わせると詳細情報を取得できます。リンクとスイッチは色分けされています。パフォーマンスコレクションと SNMP トラップを有効にして、トポロジの情報を表示します。

次の表に、リンクとスイッチに関連する色の説明を示します。

Table 7: **色の説明**

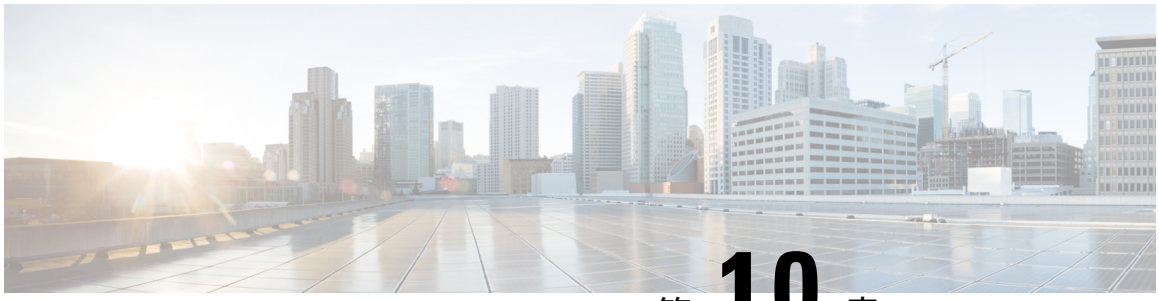
カラー	名前	説明
ブルー（ライト）	レベル 5	高使用率 tx-datarate >= 80%
緑	レベル 4	は見つかりませんでした
赤	レベル 3	クレジット損失回復
オレンジ	レベル 2	ドロップ
黄（ダーク）	レベル 1.5	txwait >= 30%

カラー	名前	説明
黄（薄）	レベル 1	txwait < 30%
グレー（ライト）	データがありません	データがありません

スイッチの色は、スイッチへのリンクで検出される最高レベルのを表します。最大値は 3、最小値は 1 です。過剰使用の場合は、スイッチは 2 色になります。スイッチの右半分のライトブルーは、過剰使用を表します。スイッチの数字は、が発生しているFポートの数を表します。数字の周りの色は、スイッチのFポートで検出される最高レベルのを表します。スイッチをクリックすると、の詳細が表示されます。

リンクのを表すために、2 本の平行線が使用されています。リンクは双方向であるため、各方向には、の最高レベルを表す色があります。リンクにカーソルを合わせると、送信元と接続先のスイッチとインターフェイス名が表示されます。リンクをクリックすると、そのリンクのみに関連するデータが表示されます。

Note リンクが持つことができる最高のレベルは、**[レベル 4（Level 4）]** です。リンクの有効な色は、緑、赤、オレンジ、黄 (ダーク)、黄 (ライト)、グレー (ライト) です。



第 10 章

ホストパスの冗長性

ホストパスの冗長性

SAN ホストパスの冗長性チェックでは、非冗長ホストストレージパスを表示できます。これは、エラーを修正するための解決策とともに、ホストエンクロージャのエラーを特定するのに役立ちます。

（注） 検出されたすべてのファブリックにライセンスが必要です。そうでない場合、この機能はCisco Nexusダッシュボード ファブリック コントローラ Web クライアントで無効になります。この機能を無効にすると、ライセンスのないファブリックが検出されたことを示す通知が表示されます。

[SAN] > [ホストパスの冗長性（Host Path Redundancy）] を選択します。

このセクションは、次のトピックで構成されています。

診断テスト

手順

ステップ 1 **[SAN] > [Host Path Redundancy（ホストパス冗長性）] > [Diagnostic Test（診断テスト）]** を選択します。

ステップ 2 **[診断テスト（Diagnostic Test）]** タブで、チェックボックスを使用してホスト冗長性のオプションチェックを選択します。

ステップ 3 チェッカーの定期的な実行を有効にするには、**[24 時間ごとにテストを自動的に実行する（Automatically run tests every 24 hours）]** チェック ボックスをオンにします。チェッカーは、サーバーが起動してから 10 分後から 24 時間ごとに実行されます。

ステップ 4 **[Limit by VSANs（VSAN による制限）]** チェックボックスをオンにして、**[包含（inclusion）]** または **[除外（exclusion）]** を選択します。テキストフィールドに VSAN または VSAN 範囲を入力して、冗長性チェックからVSANに属するホストエンクロージャを含めるかスキップします。

ステップ 5 他のオプションのチェックをオンにして、関連するチェックを実行します。

ステップ 6 **[結果をクリア（Clear Results）]** をクリックして、表示されているすべてのエラーをクリアします。

ステップ 7 **[今すぐテストを実行（Run Tests Now）]** をクリックして、いつでもチェックを実行します。

ステップ 8 結果は、**[診断テスト（Diagnostic Test）]** タブの隣にある関連するタブに表示されます。

ホストパスエラー

[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [ホストパスエラー（Hostpath Errors）] タブを選択して、ホストパス冗長性エラーテーブルを表示します。テーブルの上部には、**[良好（Good）]**、**[エラー（Errored）]**、および**[スキップ（Skipped）]**の状態のホストエンクロージャの数が色付きで表示されます。

次の表では、**[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [ホストパスエラー（Hostpath Errors）]** に表示されるフィールドについて説明します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。これらは、エラーが発生したホストエンクロージャ内の各パスの数です。
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
説明	エラーの説明を指定します。
[Fix]	エラーを修正するソリューションを指定します。エラーをポイントして、エラーを修正するソリューションを表示します。
最初の確認日時（First Seen）	エラーが最初に発生した時期を指定します。

次の表では、**[アクション（Actions）]** メニュードロップダウンリストで、**[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [ホストパスエラー（Hostpath Errors）]** に表示されるアクション項目について説明します。

アクション項目	説明
無視するホスト	テーブルから行を選択し、**[ホストを無視（Ignore Host）]** を選択して、選択した行のホストエンクロージャを除外リストに追加します。そのホストからのエラーは報告されなくなり、現在のエラーはデータベースから削除されます。
ストレージを無視する	テーブルから行を選択し、**[ストレージを無視（Ignore Storage）]** を選択して、選択した行のストレージエンクロージャを除外リストに追加します。
ホストストレージペアを無視	テーブルから行を選択し、**[ホストストレージペアを無視（Ignore Host Storage Pair）]** を選択して、選択した行のホストストレージペアエンクロージャを除外リストに追加します。
結果の消去	テーブルから行を選択し、**[結果の消去（Clear Results）]** を選択して結果をクリアします。

無視されたホスト

[SAN] > [ホストパスの冗長性（Host Path Redundancy）] > [無視されたホスト（Ignored Host）] タブを選択して、冗長性チェックによってスキップまたは無視されたホストエンクロージャのリストをスキップの理由とともに表示します。

次の表では、**[SAN] > [ホストパスの冗長性（Host Path Redundancy）] > [無視されたホスト（Ignored Host）]** に表示されるフィールドについて説明します。ホストエンクロージャを選択し、**[無視を解除（Unignore）]** をクリックしてホストを無視リストから削除し、無視することを選択したホストに関するエラーの受信を開始します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。

フィールド	説明
理由を無視する	ホストが無視された理由を指定します。 次の理由が表示される場合があります。 • **[スキップ：エンクロージャには HBA が 1 つしかありません。（Skipped: Enclosure has only one HBA.）]** • **[ホストはユーザーによって無視されました。（Host was ignored by the user.）]** • **[複数のフェデレーションサーバーによって管理されるホストポート。チェックを実行できません。（Host ports managed by more than one federated servers. Check can't be run.）]** • **[スキップ：ストレージへのパスが見つかりません。（Skipped: No path to storage found.）]**

無視されたストレージ

[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [無視されたストレージ（Ignored Storage）] タブを選択して、冗長性チェック中に無視するように選択されたストレージエンクロージャのリストを表示します。

次の表では、**[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [無視されたストレージ（Ignored Storage）]** に表示されるフィールドについて説明します。ストレージエンクロージャを選択し、**[無視の解除（Unignore）]** をクリックして、無視するリストからストレージを削除し、無視することを選択したストレージに関するエラーの受信を開始します。

フィールド	説明
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
理由を無視する	ストレージが無視された理由を指定します。

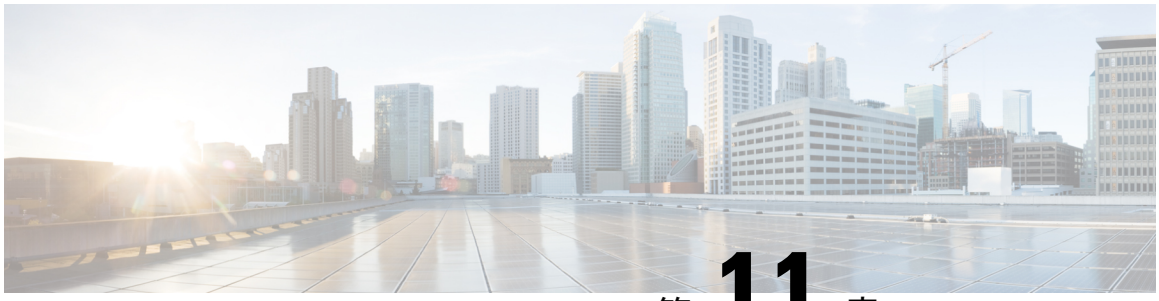
無視されたホストストレージペア

[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [無視されたホストストレージペア（Ignored Host Storage Pair）] タブを選択して、冗長性チェック中に無視するように選択されたホストストレージペアのリストを表示します。

次の表では、**[SAN] > [ホストパス冗長性（Host Path Redundancy）] > [無視されたホストストレージペア（Ignored Host Storage Pair）]** に表示されるフィールドについて説明します。行を

選択し、**[無視の解除（Unignore）]**をクリックして、ホストストレージペアを無視されたリストから削除します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
理由を無視する	ストレージが無視された理由を指定します。



第 11 章

ポート監視

ポートモニタリングポリシー

この機能により、カスタム ポート モニタリング ポリシーを Cisco SAN コントローラデータベースに保存できます。選択したカスタムポリシーを 1 つ以上のファブリックまたは Cisco MDS 9000 シリーズスイッチにプッシュできます。このポリシーは、スイッチでアクティブなポートモニタポリシーとして指定されています。

この機能は Cisco MDS 9000 SAN スイッチでのみサポートされているため、Cisco SAN コントローラのユーザーは、ポリシーをプッシュする MDS スイッチを選択できます。

Cisco SAN コントローラには、ポリシーをカスタマイズするための 12 のテンプレートが用意されています。ユーザー定義のポリシーは、Cisco SAN コントローラデータベースに保存されます。任意のテンプレートまたはカスタマイズされたポリシーを選択して、目的のポートタイプで選択したファブリックまたはスイッチにプッシュできます。

Cisco SAN コントローラリリース 12.0.1a から、新しいポートモニタリングリシー **[fabricmon_edge_policy]** が追加されました。

（注） ユーザー定義のポリシーのみを編集できます。

次の表では、Cisco ファブリックコントローラ**[SAN]**>**[ポートモニタリング（Port Monitoring）]** で表示されるフィールドについて説明します。

フィールド	説明
選択したポートモニタリングポリシー	このドロップダウンリストには、ポリシーの次のテンプレートが表示されます。 • Normal_edgePort • Normal_allPort • Normal_corePort • Aggressive_edgePort • Aggressive_allPort • Aggressive_corePort • Most-Aggressive_edgePort • Most-Aggressive_allPort • Most-Aggressive_corePort • デフォルト • slowdrain • fabricmon_edge_policy
論理型	選択したポリシーのポートのタイプを指定します。使用可能なポートタイプは次のとおりです。 • コア • エッジ • すべて
保存	ユーザー定義ポリシーの変更を保存できます。 （注） デフォルトテンプレートの構成変更を保存することはできません。

フィールド	説明
名前を付けて保存	既存のポリシーを別の名前の新しいポリシーとして保存できます。 これにより、テンプレートにカスタムポリシーとして別の項目が作成されます。カスタマイズされたポリシーは、このカテゴリの下に保存されます。 ポリシーの編集中に **[名前を付けて保存（Save As）]** をクリックすると、カスタマイズされたポリシーが保存されます。 新しいポリシーを作成するには。 • 必要なポートモニタリングポリシーを選択し、**[名前を付けて保存（Save As）]** をクリックします。 **[新しいポートモニタリングポリシー（New Port Monitoring Policy）]** ウィンドウが表示されます。 • 新しいポリシー名を入力し、必要な論理タイプを選択して、**[保存（Save）]** をクリックします。
Delete	すべてのユーザー定義のポリシーを削除できます。

フィールド	説明
スイッチにプッシュ	

フィールド	説明
	ファブリックまたはスイッチを選択し、選択したポリシーを目的のポートタイプにプッシュできます。 次のポリシーは、コアポリシータイプを選択します。 • Normal_corePort • Aggressive_corePort • Most-Aggressive_corePort 次のポリシーは、エッジポリシータイプを選択します。 • Normal_edgePort • Aggressive_edgePort • Most-Aggressive_edgePort • fabricmon_edge_policy • slowdrain 次のポリシーは、すべてのポリシータイプを選択します。 • Normal_allPort • Aggressive_allPort • Most-Aggressive_allPort • デフォルト パラメータを選択し、**[プッシュ（Push）]** をクリックして、ファブリック内のスイッチにポリシーをプッシュします。 リリース 12.0.1a の SAN コントローラの場合、事前定義されたポートとは別に、選択したポリシーに必要なポートタイプを変更できます。 • 必要なポリシーを選択し、**[スイッチにプッシュ（Push to Switches）]** をクリックします。 **[スイッチにプッシュ（Push to Switches）]** ポップアップウィンドウが表示されます。 • 必要なポートタイプを選択し、**[プッシュ（Push）]** をクリックします。 同じまたは共通のポートタイプを持つアクティブなポリシーがある場合、push コマンドは選択したデバイスに同じポリシーを設定します。このポリシーは、既存のアクティブポリシーを同じまたは共通のポートタイプに置き換えます。

フィールド	説明
	既存のポリシーを置き換える警告メッセージが表示されます。**[確認（Confirm）]** をクリックしてポリシーを書き換えます。 スイッチにプッシュされたポリシーの確認メッセージが表示されます。[ログの表示（View logs）] をクリックしてスイッチのログの詳細を表示するか、**[OK]** をクリックしてホームページに戻ります。 ポリシーの編集中に **[スイッチにプッシュ（Push to Switches）]** をクリックすると、カスタマイズされたポリシーは保存されません。 SAN コントローラは、FPIN または DIRL ポートガードを使用してエッジ論理タイプポリシーをプッシュしてアクティブ化すると、ファブリック パフォーマンス モニタ（FPM）機能を有効にします。 （注） FPIN または DIRL 機能カウンタを使用するポリシーに Cisco MDS 9250i マルチサービス ファブリック スイッチを選択すると、警告ウィンドウが表示されます。
説明	詳細情報を表示するには、説明の横にある「i」アイコンにポインタを移動します。 SAN コントローラ リリース 12.0.1a 以降、次の新しいカウンタが導入されました。 • Rx データレートバースト • Tx データレートバースト • SFP Rx 電力低下警告 • SFP Tx 電力低下警告 • 入力エラー
上昇しきい値	カウンタタイプの上限しきい値を指定します。
上昇イベント	上昇しきい値に達したとき、または超えたときに生成されるイベントのタイプを指定します。
下降しきい値	カウンタタイプの下限しきい値を指定します。
アラート	ポートのアラートのタイプを指定します。アラートは、syslog、rmon、および oblf です。 アラートは、リリース 8.5(1) の Cisco MDS スイッチにのみ適用されます。
ポーリング間隔	カウンタ値をポーリングする時間間隔を指定します。

フィールド	説明
警告しきい値	上限しきい値よりも低く、下限しきい値よりも高いオプションのしきい値を設定して、syslog を生成できます。 範囲は 0 ～ 9223372036854775807 です。
ポートガード	ポートガードを有効にするか無効にするかを指定します。値は、false、flap、または errordisable にすることができます。デフォルト値は「false」です。 Cisco SAN コントローラリリース 12.0.1a から、新しいポートガード **FPIN**、**DIRL**、および **cong-isolate-recover** がエッジポートタイプにのみ追加されます。 （注） DIRL は、Cisco SAN コントローラ 12.0.1a のプレビュー機能です。実稼働環境での使用は推奨されません。
輻輳信号警報	ポート間の輻輳の増加を示します。これは、**TxWait (%)** カウンタでのみ使用できます。
輻輳信号 アラーム	ポート間のクリティカルな輻輳を示します。これは、Tx-Wait カウンタでのみ使用できます。
モニターリング	true または false の値を示します。
編集	クリックして各行の上記の詳細を編集し、チェックマークをクリックして構成の変更を保存します。 （注） 各行の構成を編集するときに、[保存（Save）] および [名前を付けて保存（Save As）] オプションを使用して保存された構成の変更を上書きできます。

SFP カウンタの設定

Cisco MDS NX-OS リリース 8.5(1) 以降、SFP カウンタを使用すると、SFP の 送信電力および受信電力の警告下限しきい値を設定できます。これらのしきい値が設定値を下回ると、syslog を受信します。

SFP は 10 分に 1 回モニタリングされます。上昇しきい値は、受信電力または送信電力回数のカウントです。この電力時間は、SFP の受信電力または送信電力低警告しきい値にパーセンテージを掛けた値以下となります。したがって、10 分ごとに上昇しきい値を増やすことができます。ポーリング間隔の 600 倍を超える上昇しきい値を設定すると、エラーが表示されます。

たとえば、ポーリング間隔が 1200 の場合、上昇しきい値は 2（1200/600）になり、2 より大きくする必要があります。SFP カウンタはデフォルトポリシーに含まれておらず、使用可能なアラートアクションは syslog のみです。port monitor counter コマンドを使用して、ポーリング間隔を設定できます。

次のいずれかを選択して SFP カウンタを設定し、次のオプションを実行できます。

- 警告下限しきい値のパーセンテージを 100% に設定すると、Rx 電力が SFP の Rx 電力警告下限しきい値以下の場合に、このカウンタがトリガーされます。
- 警告の下限しきい値のパーセンテージを 100% 未満に設定すると、Rx 電力が SFP の Rx 電力の警告下限しきい値を超えると、このカウンタがトリガーされます。
- 低警告しきい値のパーセンテージを 100% より大きく設定すると、Rx 電力が SFP の Rx 電力低警告しきい値（低警告と低アラームの間）を下回ると、このカウンタがトリガーされます。

SFP カウンタは次のとおりです。

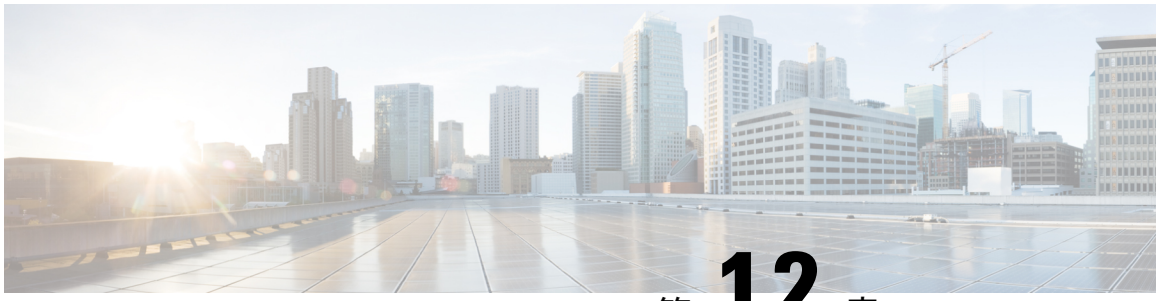
- **sfp-rx-power-low-warn**

  SFP のポートが SFP の Rx 電力の警告下限しきい値のパーセンテージに達した回数を指定します。このしきい値は、SFP のタイプ、速度、および製造元によって異なり、show interface transceiver details コマンドで表示されます。この値は、個々の SFP の Rx 電力警告下限しきい値のパーセンテージであり、完全な値ではありません。このパーセンテージを 50 ～ 150% の範囲で構成して、Rx 電力の警告下限しきい値未満または受信電力警告警告の下限しきい値を超える値でアラートを送信できるようにすることができます。これは完全な値であり、50% から 150% の間で変化します。警告下限しきい値は、SFP の実際の警告下限しきい値に指定されたパーセンテージを掛けた値として計算されます。Rx 電力が警告下限しきい値以下の場合、このカウンタが増分します

- **sfp-tx-power-low-warn**

  SFP のポートが SFP の送信電力の警告下限しきい値の割合に達した回数を指定します。このしきい値は、SFP のタイプ、速度、および製造元によって異なり、show interface transceiver details コマンドで表示されます。この値は、個々の SFP の Tx 電力低警告しきい値のパーセンテージであり、完全な値ではありません。このパーセンテージを 50 ～ 150% の範囲で構成して、Tx 電力の警告下限しきい値未満または送信電力警告警告の下限しきい値を超える値でアラートを送信できるようにすることができます。これは完全な値であり、50% から 150% の間で変化します。警告下限しきい値は、SFP の実際の警告下限しきい値に指定されたパーセンテージを掛けた値として計算されます。Tx 電力が警告下限しきい値以下の場合、このカウンタが増分します。

Cisco MDS NX-OS リリース 8.5(1) 以降、データレート バースト カウンタは、データレートが設定されたしきい値データレートを超える回数を 1 秒間隔でモニタリングします。数値が上昇しきい値に設定された数値を超えると、条件が満たされると、設定されたアラートアクションが実行されます。データレート バースト カウンタは毎秒ポーリングされます。データレート バースト カウンタは、デフォルトポリシーに含まれていません。データレート バースト カウンタの設定については、『*Cisco MDS 9000 Series Interfaces Configuration Guide*』の「*Configuring a Port Monitor Policy*」セクションを参照してください。



第 12 章

アクティブゾーン

通常ゾーン

SAN コントローラで設定されているすべての通常ゾーンを表示できます。**[SAN] > [アクティブゾーン（Active Zones）] > [通常のゾーン（Regular Zones）]** タブを選択します。次の表では、この画面のフィールドについて説明します。

表 *8 :*

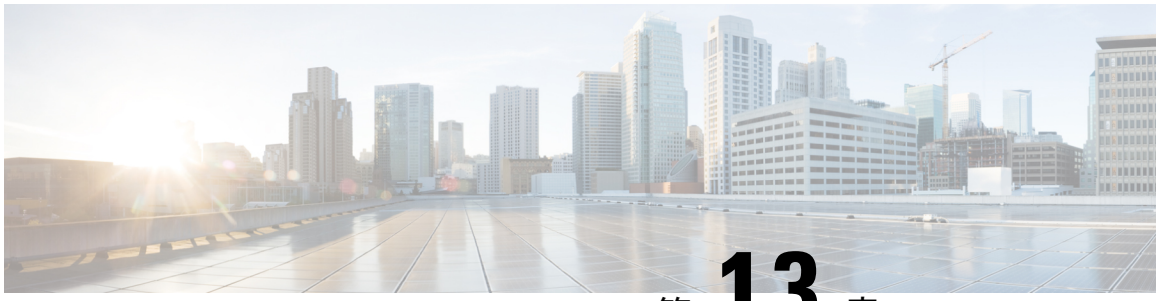
フィールド	説明
グループ	ファブリック名を指定します。
VSAN	このゾーンで設定されている VSANS の数を指定します。
ゾーン セット	ゾーンが属するゾーンセットの名前を指定します。
ゾーン	このメンバーが存在するゾーンを表示します。
スイッチインターフェイス/WWN	ゾーンメンバーが接続されているスイッチのスイッチインターフェイスまたは WWN を指定します。
PWWN	スイッチに関連付けられた pWWN を指定します。
メンバー名	ゾーンメンバーの名前を表示します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。WWN、FCID、fcAlias、iSCSI などのゾーン分割のタイプで検索できます。

IVR ゾーン

SAN コントローラで設定されているすべての IVR ゾーンを表示できます。**[SAN] > [アクティブゾーン（Active Zones）] > [IVR ゾーン（IVR Zones）]** タブを選択します。次の表では、この画面のフィールドについて説明します。

表 9:

フィールド	説明
グループ	ファブリック名を指定します。
VSAN	このゾーンで設定されている VSANS の数を指定します。
ゾーン セット	ゾーンが属するゾーンセットの名前を指定します。
ゾーン	このメンバーが存在するゾーンを表示します。
スイッチインターフェイス/WWN	ゾーンメンバーが接続されているスイッチのスイッチインターフェイスまたは WWN を指定します。
PWWN	スイッチに関連付けられた pWWN を指定します。
メンバー名	ゾーンメンバーの名前を表示します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。WWN、FCID、fcAlias、iSCSI などのゾーン分割のタイプで検索できます。



第 13 章 ストレージ

ストレージ アレイ

このタブには、ストレージアレイに関する情報が表示されます。

次の表では、**[SAN] > [ストレージ（Storage ）] > [ストレージアレイ（Storage Arrays）]** に表示されるフィールドについて説明します。

フィールド	説明
storageName	ストレージ名を指定します。 **[storageName]** をクリックして、**[ストレージエンクロージャ（Storage Enclosure）]** の詳細を表示します。表示されるタブの詳細については、「storageName エンクロージャ （147 ページ）」を参照してください。
WWN	スイッチの World Wide Name（WWN）を指定します。 ファブリック検出によって検出されたストレージアレイの PWWN のみが表示されます。ただし、ストレージアレイには、ここで指定されているよりも多くのポートがある場合があります。

storageName エンクロージャ

[storageName] アイテムをクリックして、各ストレージアレイに関する詳細情報を表示します。

ストレージアレイの詳細は、検出されたアレイのタイプと、プロバイダーが SMI-S 標準に準拠しているかどうかによって異なります。アレイをクリックして、概要タブから始まるインベントリページ、およびアレイのタイプに基づいた他のコンテキスト固有のタブを読み込みします。

以下のドキュメントには、追加の関連情報が記載されています。

- **概要**

  この表は、プロバイダーに関する情報を提供します。ストレージアレイの**シリアル番号**、**ストレージタイプ**、およびアレイ内の**物理ディスクの数**も表示されます。

- **コンポーネント**

  このタブには、ストレージ内のすべてのコンポーネントが一覧表示されます。

  コンポーネントの**名前**をクリックして、合計ストレージ容量、使用状況の詳細、および物理ディスクの詳細を表示します。

- **プール**

  このタブには、すべてのプール、そのステータス、およびRaw容量が一覧表示されます。**[プール名（POOL Name）]** をクリックして、プールの詳細を表示します。

- **LUN**

  このタブには、ストレージアレイ内のすべてのLUNが一覧表示されます。各LUNの**LUN ID**、**WWN**、**ステータス**、および**容量**の詳細を提供します。**[LUN 名（LUN Name）]**をクリックして、各 LUN の詳細を表示します。**[LUN の詳細（LUN Detail）]**ビューで**[ホスト LUN アクセス（Host LUN Access）]**情報を表示することもできます。

  ホストLUNアクセステーブルの**ホストポートPWWN**、**ホストインターフェイス**、**ゾーニング**、および**ストレージインターフェイス**の値は、この LUN にアクセスするホストが NDFC で検出されたファブリックの一部である場合にのみ表示されます。

- **ホスト**

  このタブには、選択したストレージ内のすべてのホストが一覧表示されます。これは、ストレージアレイ内の各ホストの**ホスト名**、**ノードWWN**、および**WWN**の詳細を提供します。**[ホスト名（Host Name）]**をクリックして、ホストに関する詳細を表示します。**[ホストの詳細（Host Detail）]** ビュー内の **[LUN]** タブと **[ポート（Ports）]** タブで、関連する詳細を表示できます。

  LUN タブ > ホスト LUN アクセス テーブルの**ホストインターフェイス**、**ゾーン分割**、および**ストレージインターフェイス**の値は、この LUN にアクセスするホストが NDFC で検出されたファブリックの一部である場合にのみ表示されます。

  ホストポートテーブルの**ファブリック**と**ホストインターフェイス**の値は、**ホストポート WWN** が NDFC で検出されたファブリックの一部である場合にのみ表示されます。

- **プロセッサ**

  このタブには、すべてのプロセッサとそのステータスが一覧表示されます。各プロセッサのアダプタの数も表示されます。詳細を表示するには、**[プロセッサ名（Processor Name）]** をクリックします。

- **ポート**

このタブには、ストレージアレイ内のすべてのポートが一覧表示されます。ポートの詳細を表示するには、**ポート名**をクリックします。

ホスト LUN アクセステーブルの**ホストインターフェイス**、**ゾーン分割**、および**ストレージインターフェイス**の値は、**LUN ID** 列の LUN にアクセスするホストが NDFC で検出されたファブリックの一部である場合にのみ表示されます。

ストレージ SMI-S プロバイダー

このタブには、SMI-S プロバイダーの情報が表示されます。

次の表では、**[SAN] > [ストレージ（Storage ）] > [ストレージ SMIS プロバイダー（Storage SMIS Provider）]** に表示されるフィールドについて説明します。

フィールド	説明
ベンダー	ベンダーを指定します。 Cisco NDFC は、次のベンダーをサポートしています。 • EMC • NetApp • IBM • HDS • PureStorage • HP • その他
プロバイダーの URL	SMI-S プロバイダーの URL を指定します。
名前空間	名前空間を指定します。
相互運用名前空間	相互運用名前空間を指定します。
[ポート（Port）]	ポートを指定します。
ステータス	ステータスを指定します。
セキュア	安全な接続かどうかを指定します。
検出ステータス	検出ステータスを指定します。
最終更新時刻	最後に更新された日時を示します。

次の表で、**SAN > [ストレージ（Storage）] > [ストレージ SMIS プロバイダー（Storage SMIS Provider）]** で表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
プロバイダの追加	SMI-S プロバイダーを追加します。手順については、「SMI-S プロバイダーの追加 （150 ページ）.
プロバイダの編集	テーブルからプロバイダーを選択し、**[プロバイダーの編集（Edit Provider）]** を選択してプロバイダー情報を更新します。
プロバイダーの削除	テーブルからプロバイダーを選択し、**[プロバイダーの削除（Delete Provider）]** を選択してプロバイダーを削除します。
プロバイダーの再検出	テーブルからプロバイダーを選択し、**[プロバイダーの再検出（Rediscover Provider）]** を選択して変更をスキャンします。これにより、通常の定期的なポーリング以外で検出サイクルがトリガーされます。
プロバイダーの消去	テーブルからプロバイダーを選択し、**[プロバイダーの消去（Purge Provider）]** を選択してプロバイダー情報を消去します。これにより、存在しなくなった要素が検出から削除されます。

SMI-S プロバイダーの追加

Cisco Nexusダッシュボード ファブリック コントローラ Web UI から SMI-S プロバイダーを追加するには、次の手順を実行します。

手順

ステップ 1 **[SAN] > [ストレージ（Storage）] > [ストレージ SMIS プロバイダー（Storage SMIS Provider）]** を選択します。

[ストレージ SMIS プロバイダー（Storage SMIS Provider）] タブが表示されます。

ステップ 2 **[アクション（Actions）]** メニューのドロップダウンリストをクリックし、**[プロバイダーの追加（Add Provier）]** をクリックします。

[SMI-S の追加（Add SMI-S）] ウィンドウが表示されます。

ステップ 3 ドロップダウンを使用して **[ベンダー（Vendor）]** を選択します。

サポートされているすべてのベンダーがドロップダウンリストに表示されます。ドロップダウンの **[その他（Other）]** のベンダーオプションを使用して、「ベストエフォート」ハンドラーを通じて、より多くの SMI-S ストレージベンダーが検出されます。

（注） SMI-S ストレージ検出用のデータソースを追加する前に、少なくとも 1 つの有効な Nexusダッシュボード ファブリック コントローラ ライセンスをプロビジョニングする必要があります。

ステップ 4 **SMI-S サーバーの IP**、**ユーザー名**、および**パスワード**を指定します。

ステップ 5 **名前空間**と**相互運用名前空間**を指定します。

ステップ 6 デフォルトでは、**ポート**番号は事前に入力されています。

[セキュア（Secure）] チェックボックスをオンにすると、デフォルトのセキュアポート番号が入力されます。

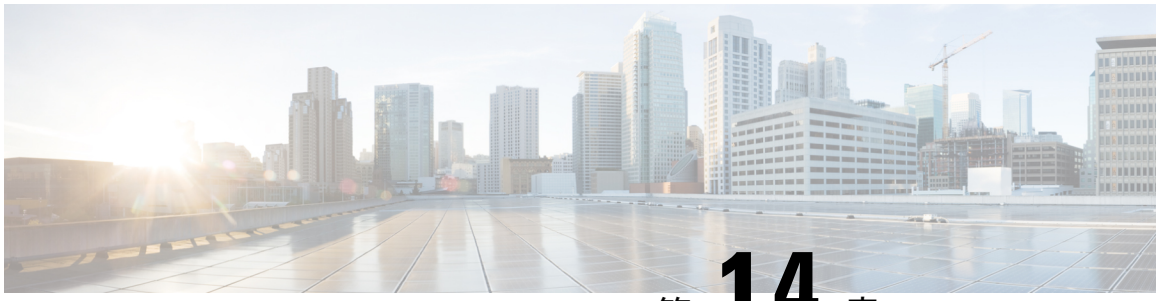
EMC で**セキュア**モードを使用する場合、デフォルト設定は相互認証です。詳細については、トラストストアへの SSL 証明書の追加に関する EMC のドキュメントを参照してください。また、*Security_Settings.xml* 構成ファイルで SSLClientAuthentication 値を *None* に設定し、ECOM サービスを再起動することもできます。

ステップ 7 [Add] をクリックします。

ログイン情報が検証され、ログイン情報が有効な場合はストレージの検出が開始されます。ログイン情報チェックに失敗した場合は、有効なログイン情報を入力するように求められます。

第 II 部

仮想的な管理



第 14 章

ゾーン分割

ゾーン分割

ゾーン分割により、ストレージ デバイス間またはユーザー グループ間でアクセス コントロールの設定ができます。ファブリックで管理者権限を持つユーザーは、ゾーンを作成してネットワークセキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。

SAN コントローラ リリース 12.0.1a 以降、通常のゾーンと IVR ゾーンが単一のゾーン分割ページにマージされます。

（注） Web UI のゾーン分割にデバイスエイリアスが使用されている場合、エンドデバイスはファブリックにログインする必要があるため、Web GUI はデバイスエイリアスを使用してゾーン分割を設定できます。エンドノードにログインしていない場合は、ゾーン分割に PWWN を使用できます。

次の表では、SAN コントローラの **[仮想管理（Virtual Management）]** > [ゾーン分割（Zoning）] タブに表示されるフィールドとアイコンについて説明します。

フィールド	説明
ゾーン分割のタイプ	**[通常（Regular）]** または **[IVR]** の横にあるオプションボタンを選択して、必要なゾーン分割タイプを選択します。
ファブリック	[ファブリック（Fabric）] ドロップダウンリストから、ゾーン分割を設定または表示するファブリックを選択できます。 管理者ロールがファブリックをロックしている場合、ファブリックフィールドの隣にロックアイコンが表示されます。

フィールド	説明
VSAN	通常のゾーン分割タイプを選択して、VSAN フィールドを表示します。 VSAN ドロップダウンリストから、通常のゾーンを設定する VSAN を選択できます。
地域ID	リージョン ID フィールドを表示するには、IVR ゾーン分割タイプを選択します。 [リージョン ID（Region ID）] ドロップダウンリストから、IVR ゾーンを設定するリージョン名を選択できます。
拡張ゾーン分割	**[VSAN]** テキストフィールドの横にある **[設定（Configurations）]** アイコンをクリックして、拡張ゾーン分割ウィンドウを表示します。 （注） 拡張ゾーン分割は通常ゾーンでのみサポートされています。 詳細については、拡張ゾーン分割セクションを参照してください。
Cisco Fabric Services（CFS）	**[リージョン ID（Region ID）]** フィールドの横にある **[セットアップアシスタント（set-up assistant）]** アイコンをクリックして、CFS ウィンドウを表示します。 （注） CFS は、IVR ゾーン分割でのみサポートされます。 詳細については、CFSの項を参照してください。
スイッチ	[スイッチ（Switch）] ドロップダウンリストから、設定するスイッチを選択します。
Action	[ゾーン分割（Zoning）] フィールドで、**[アクション（Actions）]** をクリックして以下を表示します。 • 変更 • データベース • サーバーキャッシュを消去 • 検出同期

フィールド	説明
変更	[ゾーン分割（Zoning）] フィールドで、**[アクション（Actions）]** > **[変更（Changes）]**の順にクリックします。 • スマートゾーン分割を有効にする：すべてのスイッチのスマートゾーン分割設定を有効にします。 • 変更のコミット：ゾーン分割設定の変更をすべてのスイッチにコミットします。このフィールドは、ゾーンが拡張モードまたはスマートモードの場合にのみ適用されます。 • 保留中の破棄：保留中の変更の破棄を実行中です。
データベース	[ゾーン分割（Zoning）] フィールドで、**[アクション（Actions）]**>**[データベース（Database）]**をクリックします。 • データベースのバックアップ：[データベースのバックアップ（Backup Database）] を選択すると、**[データベースのバックアップ（Backup Database）]** ウィンドウが表示されます。名前を入力し、**[バックアップ（Backup）]** をクリックします。 • データベースの復元：[データベースの復元（Restore Database）] を選択すると、**[データベースの復元（Restore Database）]** ウィンドウが表示されます。適切なファイルをアップロードし、**[復元（Restore）]**をクリックします。
サーバーキャッシュを消去	[ゾーン分割] エリアで、**[アクション（Actions）]** > **[サーバーキャッシュのクリア（Clear Server Cache）]**の順に選択します。 サーバー上のキャッシュをクリアします。
検出同期	[ゾーン分割（Zoning）]エリアで、**[アクション（Actions）]**> **[検出同期（Discovery Sync）]**を選択します。 ゾーン分割モジュールを検出と同期するには。

この章は、次の項で構成されています。

拡張ゾーン分割

SAN コントローラリリース 12.0.1a から、通常のゾーン分割タイプに拡張ゾーン分割機能が追加されました。

拡張ゾーン分割では、すべての設定が単一の設定セッション内で実行されます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。

ゾーン分割タイプで**[通常（Regular）]**オプションボタンを選択し、[VSAN]フィールドの横にある**[設定（Configurations）]**アイコンをクリックして、**[拡張ゾーン分割（Enhanced zoning）]**ウィンドウを表示します。

[拡張ゾーン分割（Enhanced Zoning）]ウィンドウには、次のフィールドとその説明があります。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
モード	次のいずれかのスイッチのモードを表示します。 • Basic • Enhanced
結果	次のいずれかのアクティベーション結果を表示します。 • 成功 • 失敗
以下によってロックされた設定 DB	ロックされた設定データベースのロール名を表示します。
Action	次のいずれかのスイッチのアクションを表示します。 • オペレーションなし • 変更を確定します。 • クリーンアップ 最後の列の**[編集（edit）]**アイコンをクリックして必要なアクションを選択し、[チェックマーク（check mark）]アイコンをクリックして保存します。
最後のアクション結果	最後の設定データベースのステータスを表示します。
完全な DB マージを強制する	ステータスを有効または無効に表示します。最後の列の**[編集（edit）]**アイコンをクリックして必要なアクションを選択し、[チェックマーク（check mark）]アイコンをクリックして保存します。 これを有効にすると、アクティブゾーンとローカルゾーンの両方がマージされ、VSAN のすべてのスイッチで同一になります。

フィールド	説明
続きを読む	拡張ゾーンまたはIVR CFS 対応ゾーンの場合、スイッチのゾーン分割DBに変更が加えられると、commitコマンドが発行されるまで、すべてのゾーンデータが保留中のデータベースにプッシュされます。 このフラグは、ユーザーが保留中のゾーン DB（コピー DB）または通常のゾーン DB（有効な DB）からデータを取得するのに役立ちます。 最後の列の **[編集（edit）]** アイコンをクリックして必要なアクションを選択し、[チェックマーク（check mark）] アイコンをクリックして保存します。
アクティブ化された日付	ゾーンセットがアクティブ化された日付を指定します。

SAN コントローラ Web UI の [拡張ゾーン分割（Enhanced Zoning）] ウィンドウでさまざまな操作を実行するには、次の手順を実行します。

Procedure

ステップ 1 **[仮想管理（Virtual Management）]** > **[ゾーン分割（Zoning）]**を選択し、必要な**[ゾーンタイプ（Zone Type）]**、**[ファブリック（Fabric）]**、および **[VSAN]** を選択します。

ステップ 2 **[VSAN]** フィールドの隣にある **[設定（configurations）]** アイコンをクリックします

[拡張ゾーン分割（Enhanced Zoning）] ウィンドウが表示されます。

ステップ 3 **[続きを読む（Read from）]** 列の横にある **[編集（Edit）]** アイコンをクリックして必要なデータベースを選択し、**[チェックマーク（Tick）]** アイコンをクリックして保存します。

ステップ 4 モードを基本から拡張に変更するには、**[アクション（Actions）]** > **[モードを拡張に設定（Set Mode to Enhanced）]**を選択し、**[適用（Apply）]** をクリックします。

ステップ 5 同じ手順に従って、モードを拡張から基本に設定し、**[アクション（Actions）]** > **[モードを基本に設定（Set Mode to Basic）]** を選択して、**[適用（Apply）]** をクリックします。

CFS

Cisco Fabric Service（CFS）は、IVR ゾーン分割のファブリック内で自動的に設定を同期化するための、共通のインフラストラクチャを提供します。CFS が 1 つのスイッチで設定されていて、同じプロパティを他のスイッチで送信できる場合。スイッチでIVR を有効または無効にすることができます。さらに、選択したスイッチで CFS とグローバル CFS の両方を有効または無効にすることができます。

ゾーン分割タイプで**[IVR]**オプションボタンを選択し、**[VSAN]**フィールドの隣にある**[セットアップアシスタント（set-up assistant）]**アイコンをクリックして、CFS ウィンドウを表示します。

CFS ウィンドウでは、以下のタブを表示できます。

- Control
- IVR
- Action

次の表では、**[コントロール（Control）]**タブに表示されるフィールドについて説明します。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
IVR ステータス	スイッチで IVR が有効または無効であるかを表示します。
編集	**[編集（Edit）]**アイコンをクリックしてスイッチの IVR を有効または無効にし、チェックマークをクリックして変更を保存します。
リフレッシュ	表を更新するには、**更新** アイコンをクリックします。
適用	**[適用（Apply）]**をクリックして、スイッチの変更ごとに変更を保存します。
完了	**[完了（Done ）]**をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

次の表では、**[IVR]**タブに表示されるフィールドおよび説明について記述します。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
CFS ステータス	CFS ステータスを有効にするか無効にするかを指定します。
グローバル CFS	スイッチでこの機能を有効にするか無効にするかを指定します。
続きを読む	ステータスを指定します。 • 有効な DB • DB をコピー
ロック所有者（Lock Owner）	スイッチが管理者によってロックされていることを指定します。
結合ステータス	発生したファブリックマージを指定します。
地域ID	スイッチのリージョン ID を指定します。

フィールド	説明
編集	**[編集（Edit）]** アイコンをクリックして、選択した行の [続きを読む（Read from）] 列および [リージョン ID（Region ID）] 列の変更を実行します。
適用	**[適用（Apply）]** をクリックして、スイッチの変更ごとに変更を保存します。
リフレッシュ	表を更新するには、**更新** アイコンをクリックします。
完了	**[完了（Done）]**をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

SAN コントローラ Web UI から IVR タブのスイッチでさまざまな操作を実行するには、次の手順を実行します。

Procedure

ステップ 1 スイッチを選択し、**[アクション（Actions）]** > **[コミット（Commit）]**の順に選択し、**[適用（Apply）]** をクリックして、スイッチで IVR を有効にします。

Note 変更をコミットできるのは、選択したスイッチで CFS が有効になっている場合だけです。

ステップ 2 スイッチを選択し、**[アクション（Actions）]**>**[中止（Abort）]**の順に選択し、**[適用（Apply）]** をクリックしてスイッチの IVR を無効にします。

ステップ 3 スイッチを選択し、**[アクション（Actions）]** > **[クリア（Clear）]**を選択し、**[適用（Apply）]** をクリックして、スイッチの IVR 情報をクリアします。

ステップ 4 スイッチを選択し、**[アクション（Actions）]** > **[CFS の有効化（Enable CFS）]**の順に選択し、**[適用（Apply）]** をクリックしてスイッチで CFS を有効にします。

ステップ 5 スイッチを選択し、**[アクション（Actions）]** > **[グローバル CFS を無効にする（Disable Global CFS）]**を選択し、**[適用（Apply）]** をクリックして、スイッチで CFS をグローバルに有効にします。

次の表では、**[アクション（Action）]**に表示されるフィールドおよび説明について記述します。

Actions	説明
スイッチ	スイッチの IP アドレスを指定します。
アクティブ	スイッチのアクティブステータスが true または false であることを指定します。
アクティベーション時間	アクティベーションの日付と時刻を指定します。
IVR NAT ステータス	IVR ステータスを有効にするか無効にするかを指定します。
自動検出トポロジ	自動検出トポロジステータスが true か false かを指定します

Actions	説明
編集	**[編集（Edit）]** アイコンをクリックして、選択した行の IVR NAT ステータス列と自動検出トポロジ列の変更を実行します。
地域ID	スイッチのリージョン ID を指定します。
編集	**[編集（Edit）]** アイコンをクリックして、選択した行の [続きを読む（Read from）] 列および [リージョン ID（Region ID）] 列の変更を実行します。
適用	**[適用（Apply）]** をクリックして、スイッチの変更ごとに変更を保存します。
リフレッシュ	表を更新するには、**更新** アイコンをクリックします。
完了	**[完了（Done）]**をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

ゾーンセット

選択したファブリック、VSAN、およびスイッチに基づいて、[ゾーンセット（Zoneset）] エリアには、設定されたゾーンセットとそのステータスが表示されます。ゾーンセットを作成、コピー、削除、または編集できます。さらに、ゾーンセットはアクティブ化または非アクティブ化できます。

次の表では、SAN コントローラの **[仮想管理（Virtual Management）]** > **[ゾーン分割（Zoning）]**[ゾーンセット（Zonesets）] タブに表示されるフィールドと説明について説明します。

フィールド	説明
ゾーンセット名	選択したゾーンセットの下で設定されているすべての名前を一覧表示します。
変更日	ゾーンセットが変更されているかどうかを表示します。
ゾーン	選択したゾーンセットの下に設定されているすべてのゾーンを一覧表示します。
メンバー	選択したゾーンに存在するメンバーを一覧表示します。
アクティブ化された日付	ゾーンセットがアクティブ化された日付を指定します。

手順

ステップ 1 SAN コントローラ Web UI からゾーンセットを作成するには、**[アクション（Actions）]** > **[ゾーンセットの作成（Create Zoneset）]**の順に選択します。

[ゾーンセットの作成（Create Zoneset）] ウィンドウが表示されます。

ステップ 2 ゾーンセットの有効な名前を入力し、**[ゾーンセットの作成（Create zoneset）]** をクリックします。

ゾーンセットが作成され、**[ゾーンセット（Zoneset）]** エリアに表示されます。

ステップ 3 ゾーンセットをコピー/複製するには、オプションボタンを選択し、**[アクション（Actions）]** > **[ゾーンセットのコピー/複製（Copy / Clone Zoneset）]**を選択するか、必要なゾーン名の最後の列にある **[楕円（ellipse）]** アイコンをクリックします。

[ゾーンセットのコピーまたは複製（Clone or Copy Zoneset）] ウィンドウには 2 つのオプションが表示されます。

適切なオプションボタンを選択します。次のいずれかを選択できます。

- **[コピー（Copy）]**：初期ゾーンセットのゾーンのコピーで構成される新しいゾーンセットを作成します。
  - コピーされたゾーンセットを識別するために、文字列を先頭または末尾に追加できます。**[タグ（Tag）]** フィールドに有効な文字列を入力し、**[名前の負荷（Prepend names）]** または **[名前の追加（Append names）]** オプションボタンを選択します。
  - **[複製（Clone）]**：ソースゾーンセットと同じゾーンで構成される新しい名前で新しいゾーンセットを作成します。

    [名前（Name）] フィールドに、新しいゾーンセットの有効な名前を入力します。

- **[ゾーンセットのコピー（Copy zoneset）]** をクリックして、ゾーンセットを複製またはコピーします。

  複製またはコピーされたゾーンセットが **[ゾーンセット（Zoneset）]** エリアに表示されます。

ステップ 4 ゾーンセットを削除するには、**[ゾーンセット名（Zoneset Name）]** 列の横にある [ゾーンセット（zoneset）] オプションボタンを選択し、**[アクション（Actions）]** > **[ゾーンセットの削除（Delete Zoneset）]**の順に選択します。

確認ウィンドウが表示されます。**[はい（Yes）]** をクリックして、ゾーンセットを削除します。

ステップ 5 ゾーン名を編集するには、**[ゾーンセット名（Zoneset Name）]** 列の横にあるゾーンオプションボタンを選択し、**[アクション（Actions）]** > > **[ゾーンとメンバーの編集（Edit zones & member）]**を選択するか、必要なゾーン名の最後の列にある **[楕円（ellipse）]** アイコンをクリックします。

選択したファブリックの **[ゾーンセット（Zoneset）]** ページが表示されます。

[ゾーン名（Zone Name）] 列の横にあるチェックボックスをオンにして、**[アクション（Actions）]** > **[ゾーン名の変更（Rename zone）]**の順に選択します。

ゾーンセットの新しい名前を入力します。[Rename] をクリックします。

ステップ 6 ゾーンセットを非アクティブ化するには、**[ゾーンセット名（Zoneset Name）]** 列の横にある [ゾーンセット] オプションボタンを選択し、**[アクション（Actions）]** > **[非アクティブ化（Deactivate）]**をクリックします。

確認ウィンドウが表示されます。**[はい（Yes）]** をクリックして、ゾーンセットを非アクティブにします。

ステップ 7 ゾーンセットをアクティブにするには、**[ゾーンセット名（Zoneset Name）]** 列の横にあるオプションボタンを選択し、**[アクティブ化（Activate）]** をクリックします。

[ゾーンセットの差異（Zoneset Differences）] ウィンドウには、以前にアクティブ化されてからゾーンセットに加えられた変更が表示されます。[Activate] をクリックします。

ゾーン

UI パス：**[仮想管理（Virtual Management）]**> **ゾーン分割（Zoning）**。ゾーンメンバーを選択すると、スライドインパネルが表示されます。**[起動（Launch）]** アイコンをクリックして、**[ゾーン（Zones）]** ウィンドウを表示します。

選択したゾーンセットに基づいて、そのゾーンセットの下に構成されているゾーンが **[ゾーン（Zones）]** エリアに表示されます。[ゾーン（Zones）] タブを表示するには、ゾーンセットのオプションボタンをクリックし、**[アクション（Actions）]** > **[ゾーンとメンバーの編集（Edit zones & members）]**を選択します。**[ゾーンセット（Zoneset）]** ウィンドウが表示されます。また、VSAN に有効になっているスマートゾーンがある場合にのみ、true または false が表示されます。

ゾーンを作成、コピー、削除、または複製し、名前を変更することができます。また、VSAN に有効になっているスマートゾーンがある場合にのみ、true または false が表示されます。さらに、選択したゾーンセットにゾーンを追加または削除できます。ゾーンテーブルでスマートゾーンを有効または無効にすることもできます。

ゾーンエリアには、次のフィールドとその説明があります。

フィールド	説明
属性別フィルタ処理	必要なゾーン名またはゾーンセットとメンバーを指定して検索できます。
ゾーンセットに追加	ゾーン名を選択し、**[ゾーンセットに追加（Add to zoneset）]** をクリックします。
リフレッシュ	表を更新するには、**更新** アイコンをクリックします。

フィールド	説明
Zone Name	ゾーンの名前を表示します。 ゾーン名を指定して検索できます。
ゾーンセット内	ゾーンがゾーンセットの一部であるかどうかを指定します。 ゾーンがゾーンセットの一部である場合は**true**を表示します。それ以外の場合は、**false** を表示します。 **[ゾーンセット内（In Zoneset）]** ドロップダウンリストから true または false を選択して検索できます。
メンバー	ゾーンのゾーンメンバーを指定します。 メンバーを指定して検索できます。

Procedure

ステップ 1 ゾーンを作成するには、**[仮想的な管理（Virtual Management）]** > **[ゾーン分割（Zoning）]** を選択します。

ステップ 2 **[ゾーンセット（Zonesets）]** エリアで、必要なゾーンセット名を選択します。

スライドインパネルが表示されます。

a) **[ゾーニングの編集（Edit Zoning）]** または **[起動（launch）]** アイコンをクリックして、[ゾーンセット（Zoneset ）] ウィンドウを表示します。

デフォルトでは、[ゾーン（Zones）] タブが表示されます。

ステップ 3 ゾーンを作成するには、**[アクション（Actions）]** > **[新しいゾーンの作成（Create new zone）]** を選択します。

a) **[新しいゾーンの作成（Create new zone）]** で、ゾーンの有効な名前を入力し、**[作成（Create）]** をクリックします。
b) **[新しいゾーンの作成（Create new zone）]** をクリックします。
c) **[スマートゾーン分割（Smart Zoning）]** の横にある選択ボックスを選択して、新しいゾーンのスマートゾーン分割を有効にします。

ゾーンが作成され、**[ゾーン（Zones）]** エリアに一覧表示されます。

ステップ 4 スマートゾーンを有効にするには、**[ゾーン名（Zone Name）]** の横にある必要なチェック ボックスをオンにして、**[アクション（Actions）]** > **[スマート ゾーンを有効にする（Enable smart zoning）]**を選択します。

スマートゾーン列は、VSANでスマートゾーン分割が有効になっている場合にのみ表示できます。

ステップ 5 スマートゾーンを無効にするには、**[ゾーン名（Zone Name）]** の横にある必要なチェックボックスをオンにして、**[アクション（Actions）]**、>**[スマートゾーンを無効にする（Disable smart zoning）]**の順に選択します。

ステップ 6 ゾーンを複製するには、**[構成（Configure ）] > [SAN] > [ゾーン分割（Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** オプションボタンを選択して **[ゾーンの複製（Clone Zone）]** アイコンをクリックします。

[ゾーンの複製（Clone Zone）] ウィンドウが表示されます。

a) [名前（Name）] フィールドに、新しいゾーンセットの有効な名前を入力します。
b) **[クローン（Clone）]** をクリックして、ゾーンを複製します。

複製されたゾーンが **[ゾーン（Zones）]** エリアに表示されます。

ステップ 7 ゾーンセットからゾーンの名前を変更するには、**[ゾーン名（Zone Name）]** の横にある必要なチェック ボックスをオンにして、**[アクション（Actions）]**、>**[ゾーン名の変更（Rename zone）]**の順に選択します。

[名前（Name）] フィールドに、ゾーンの新しい名前を入力して、**[名前の変更（Rename）]** をクリックします。

ステップ 8 ゾーンセットからゾーンを削除するには、**[ゾーン名（Zone Name）]** の横にある必須チェックボックスをオンにして、**[アクション（Actions）]**、>**[ゾーンセットから削除（Remove from zoneset）]**の順に選択します。

選択したゾーンセットからゾーンが削除されます。ゾーン名の横にある緑色のチェックマークが消え、ゾーンがゾーンセットから削除されたことを示します。

ステップ 9 ゾーンセットからゾーンを削除するには、**[ゾーン名（Zone Name）]** の横にある必要なチェックボックスをオンにして、**[アクション（Actions）]**、>**[ゾーンの削除（Delete zone）]**の順に選択します。

単一または複数のゾーンを選択して、すぐに削除できます。

Note 選択したゾーンセットのメンバーであるゾーンは削除できません。ゾーンを削除するには、ゾーンセットからゾーンを削除します。

FC エイリアス

ナビゲーションパス：**仮想管理 > > ゾーン分割 > ゾーンセット > メンバー**

SAN コントローラリリース 12.0.1a 以降、FC エイリアス機能は通常のゾーンでサポートされます。これは、1 つ以上の pWWN を必要な名前に関連付けるために使用されます。ゾーンメンバーを追加すると、FC エイリアスを追加したり、既存の FC エイリアスを削除したりできます。[FC エイリアス（FC Aliases）] タブには、以下のフィールドが表示されます。

- [FC エイリアス（FC Aliases）] : FC エイリアスの名前を指定します。
- [メンバー（Member）] : FC エイリアスに関連付けられたメンバーを指定します。

FC エイリアス操作を行うには、次の手順を実行します。

Procedure

ステップ 1 **[仮想的な管理（Virtual Management）]** > **[通常ゾーン（Regular Zones）]**を選択し、必要なゾーンセット名をクリックします。

スライドイン パネル ウィンドウが表示されます。

ステップ 2 **[ゾーン分割の編集（Edit Zoning）]** または **[起動（launch）]** アイコンをクリックして、**[ゾーンセット（Zoneset）]** ページを表示します。

ゾーンセットウィンドウが表示されます。

ステップ 3 **[FC エイリアス（FC Aliases）]** タブをクリックして、[FC エイリアス（FC Aliases）] エリアを表示します。

ステップ 4 新しい FC エイリアスを作成するには、**[アクション（Actions）]** > **[新しい FC エイリアスの作成（Create new FC Alias）]** の順に選択します。

[新しい FC エイリアスの作成（Create new FC Alias）] ウィンドウが表示されます。

a) テキストフィールドに有効な名前を入力し、**[FC エイリアスの作成（Create FC Alias）]** をクリックします。

FC エイリアスが作成され、[FC エイリアス（FC Aliases）] エリアに一覧表示されます。

ステップ 5 新しい FC エイリアスを削除するには、**[FC エイリアス（FC Aliases）]** 列の横にある必要なチェック ボックスをオンにして、**[アクション（Actions）]** > **[FC エイリアスの削除（Delete FC Alias）]**の順に選択します。

メンバー

UI パス：**[仮想管理（Virtual Management）]** > **[ゾーン分割（Zoning）]** > **[ゾーンセット（Zon Sets）]** > **[メンバー（Members）]**

選択したゾーンセットとゾーンに基づいて、**[メンバー（Members）]**エリアにゾーンメンバーとそのステータスが表示されます。メンバーの詳細を表示するには、**[属性別フィルタ処理（Filter by attributes）]** テキストフィールドに必要なフィールド名を入力します。

メンバーエリアには、次のフィールドとその説明があります。

フィールド	説明
Parent	ゾーンメンバーの名前を表示します。 ゾーン名を指定して検索できます。
メンバー	ゾーンのメンバー名を表示します。

フィールド	説明
スイッチ	ゾーンメンバーがリンクされているスイッチを指定します。 スイッチを指定して検索できます。
インターフェイス	ゾーンメンバーが接続されているインターフェイスを指定します。 インターフェイスを指定して検索できます。
ステータス	ゾーンの状態を指定します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。 WWN、FCID、FC エイリアス、または iSCSI、FWWN、デバイスエイリアス、IP サブネットなどのゾーン分割のタイプで検索できます。
FCID	ゾーンメンバーに関連付けられた FCID を指定します。 ゾーンメンバーに関連付けられている FCID を指定して検索できます。
pWWN	スイッチの pWWN を指定します。 スイッチの WWN を指定して検索できます。

ゾーンセットのメンバーを追加または削除できます。さらに、既存のメンバーを追加したり、既存の FC エイリアスをメンバーに追加したりすることもできます。

SAN コントローラ Web UI から、**[仮想管理（Virtual Management）]**>**[ゾーン分割（Zoning）]**>**[ゾーンセット（Zoneset）]**>**[メンバー（Members）]**を選択して、**[ゾーンセット（Zoneset）]** ウィンドウのメンバーエリアを表示します。

ゾーンセットとゾーンを選択して、ゾーンメンバーのリストを表示します。

Procedure

ステップ 1 新しいメンバーを作成するには、**[メンバー（Members）]** 領域で、**[アクション（Actions）]**>**[新しいメンバーの作成（Create new member）]**の順に選択します。

[新しいメンバーの作成と追加（Create and Add a new Member）] ウィンドウで、適切なゾーンのオプションボタンを選択します。

テキストフィールドに有効な名前を入力し、**[メンバーの作成（Create Member）]** をクリックします。

オプションボタンセクションによるゾーンに基づいて、新しい名前は、すべてのゾーンではなく、選択されたゾーンのみに付けられます。たとえば、WWN ゾーンを選択した場合、テキストフィールドの名前は WWN ゾーンの名前です。同様に、**[ドメインとポートゾーン（Domain & Port zone by）]** を選択すると、ドメイン ID 番号とスイッチインターフェイス名になります。

[新しいメンバーの作成（Create new Member）] では、現在ファブリックに存在しないゾーンにメンバーを追加できます。この機能は、デバイス検出ですべてのデバイスが検出されなかった場合に利用できます。追加可能な機能を使用すると、検出されたデバイスをゾーンに追加できます。

ステップ 2 ゾーンメンバーを削除するには、**[親（Parent）]** 列の横にあるチェックボックスをオンにして、**[アクション（Actions）]** > **[ゾーンからメンバーを削除（Remove Member from zone(s)）]** をクリックします。

インスタンス内の複数のゾーンを選択して削除できます。

ステップ 3 既存のメンバーを追加するには、**[アクション（Actions）]** > **[既存のメンバーの追加（Add existing members）]**の順に選択します。

[既存のメンバーの追加（Add existing members）] ウィンドウが表示されます。

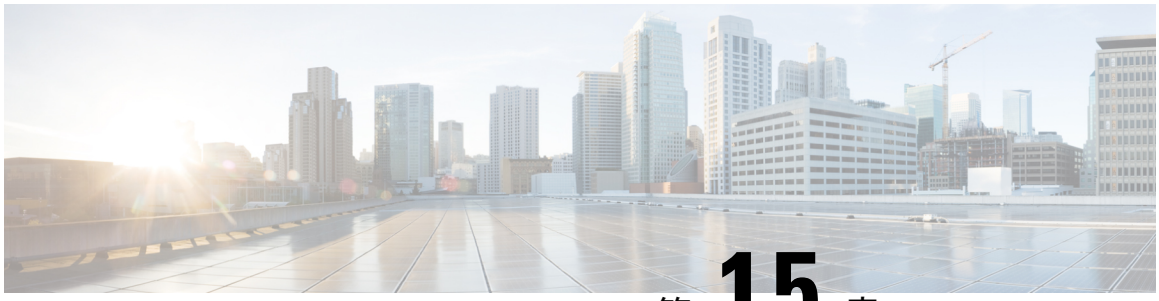
このウィンドウには、次のフィールドとその説明があります。

フィールド	説明
Zone By	**[Zone by]** 機能は、デバイス WWN またはデバイスエイリアスを使用して、デバイスをゾーンに追加する必要があるかどうかを決定します。 **[Zone by**：**エンドポート（Zone By: End Ports）]** を選択した場合、デバイスは WWN によってゾーンに追加されます。 同様に、デバイスエイリアスと FC エイリアスの場合、デバイスはそれぞれデバイスエイリアスと FC エイリアスによってゾーンに追加されます。選択した Zone by に基づいて、デバイスが表示されます。
メンバー名	ゾーンの名前を表示します。 ゾーン名を指定して検索できます。
Type	スイッチがストレージまたはホストであることを指定します。
スイッチ	ゾーンメンバーがリンクされているスイッチを指定します。 スイッチを指定して検索できます。
インターフェイス	ゾーンメンバーが接続されているインターフェイスを指定します。 インターフェイスを指定して検索できます。
pWWN	スイッチの pWWN を指定します。 スイッチの pWWN を指定して検索できます。
VSAN	ゾーンメンバーが属する VSAN を指定します。

ステップ 4 オプションで適切な **[Zone by]** を選択し、必要な **[メンバー名（Member Name）]**を選択します。

ステップ 5 **[メンバーの追加（Add Members）]** をクリックします。

Note 複数のゾーンを選択できます。ゾーンテーブルで現在選択されているすべてのゾーンのリストを示すダイアログが表示されます。



第 15 章

VSAN

VSAN

Cisco Nexusダッシュボード ファブリック コントローラ の仮想 SAN（VSAN）を構成および管理できます。メニューから、**[仮想的な管理（Virtual Management）] > [VSANS]** を選択して、VSAN 情報を表示します。 検出されたファブリックの VSAN を、**[管理可能（Manageable）]** または**継続的に管理（Manage Continuously）**ステータスで表示または設定できます。選択したファブリックでは、VSAN スコープツリーが左側のパネルに表示されます。

Cisco データセンタースイッチおよび Cisco MDS 9000 シリーズ スイッチで仮想 SAN（VSAN）を使用すると、ファイバ チャネル ファブリックでより高度なセキュリティと高い安定性を得ることができます。VSANは同じファブリックに物理的に接続されたデバイスを分離します。VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成できます。各 VSAN には最大 239 台のスイッチを組み込めます。それぞれの VSAN は、異なる VSAN で同じファイバ チャネル ID（FC ID）を同時に使用できる独立したアドレス領域を持ちます。

（注） Cisco Nexusダッシュボード ファブリック コントローラ は、一時停止された VSAN を検出せず、表示もしません。

（注） Nexusダッシュボード ファブリック コントローラ でスイッチポートの VSAN を変更すると、ポートが隔離された VSAN に関連付けられていた場合、前の VSAN 列は空白になります。

タブに表示されるすべてのフィールドの説明については、「VSAN のフィールドと説明 （183 ページ）」を参照してください。

このセクションは、次のトピックで構成されています。

VSAN に関する情報

VSAN を導入することによって、ネットワーク管理者はスイッチ、リンク、および 1 つまたは複数の VSAN を含むトポロジを 1 つ作成できます。このトポロジの各 VSAN では、SAN の動作およびプロパティが同じです。VSAN には次の特徴もあります。

- 複数の VSAN で同じ物理トポロジを共有できます。
- 同じ Fibre Channel ID（FC ID）を別の VSAN 内のホストに割り当てて、VSAN のスケーラビリティを高めることができます。
- VSAN の各インスタンスは、FSPF、ドメイン マネージャ、およびゾーン分割などの必要なすべてのプロトコルを実行します。
- VSAN 内のファブリック関連の設定は、別の VSAN 内の関連トラフィックに影響しません。
- ある VSAN 内のトラフィック中断を引き起こしたイベントはその VSAN 内にとどまり、他の VSAN に伝播されません。

VSAN がアクティブの状態で、最低 1 つのポートがアップの状態であれば、VSAN は動作ステートにあります。このステートは、トラフィックがこの VSAN を通過できることを示します。このステートは設定できません。

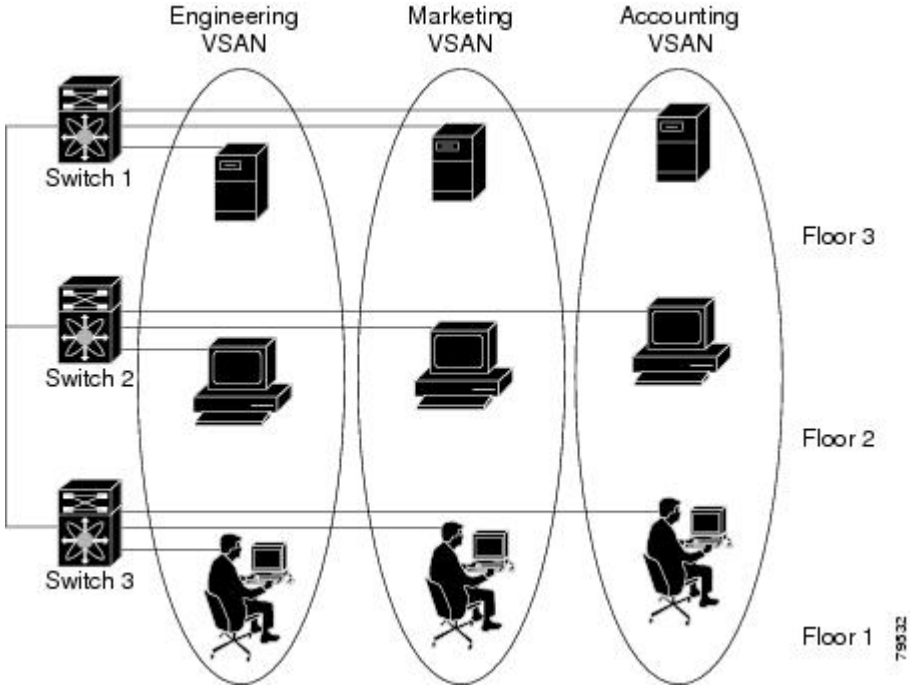
相互運用性により、複数ベンダー製品間の相互接続が可能になっています。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。最大 8 つの VSAN で FICON をイネーブルできます。

ここでは VSAN について説明します。具体的な内容は次のとおりです。

VSAN トポロジ

次の図は、各フロアに 1 つずつ、3 つのスイッチがあるファブリックを示しています。スイッチと接続された装置の地理的な配置は、論理VSANの区分けには依存しません。VSAN間では通信できません。各 VSAN 内では、すべてのメンバが相互に対話できます。

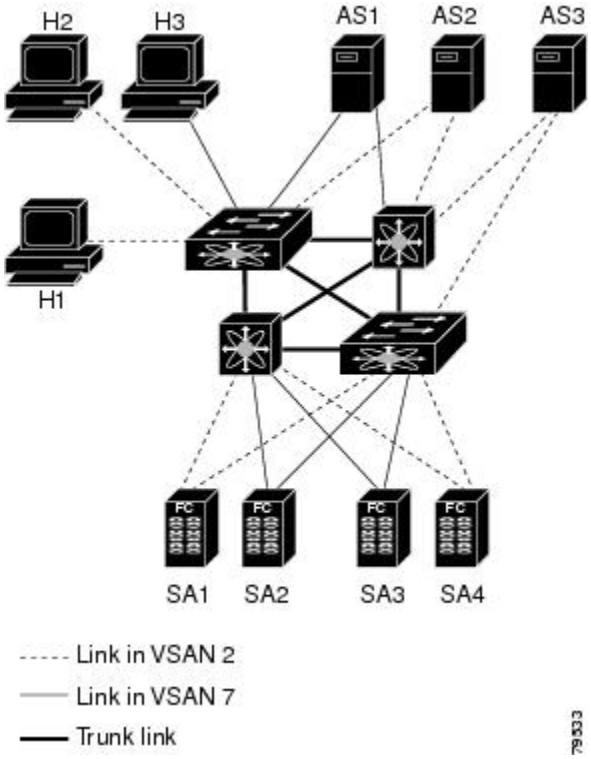
図 *8 :* 論理 *VSAN* の区分け



以下に、VSAN 2（破線）と VSAN 7（実線）の 2 つの定義済み VSAN からなるファイバ チャネル スイッチングの物理インフラストラクチャを示します。VSAN 2 には、ホスト H1 と H2、アプリケーション サーバー AS2 と AS3、ストレージ アレイ SA1 と SA4 が含まれます。VSAN 7 は、H3、AS1、SA2、および SA3 と接続します。

このネットワーク内の 4 つのスイッチは、VSAN 2 と VSAN 7 の両方のトラフィックを伝送するトランク リンクによって相互接続されます。VSAN 2 と VSAN 7 の両方のスイッチ間トポロジは同じです。これは要件ではないため、ネットワーク管理者は特定のリンクで特定の VSAN をイネーブルにして別の VSAN トポロジを作成できます。

図 *9 : 2* つの *VSAN* の例



VSANがもしなければ、SANごとに別個のスイッチとリンクが必要です。VSANをイネーブルにすることによって、同一のスイッチとリンクが複数のVSANで共有されることがあります。VSANでは、スイッチ精度ではなく、ポート精度でSANを作成できます。上の図では、VSANが物理 SAN で定義された仮想トポロジを使用して相互に通信するホストまたはストレージデバイスのグループであることを表しています。

このようなグループを作成する基準は、VSAN トポロジによって異なります。

- VSAN は、次の条件に基づいてトラフィックを分離できます。
  - ストレージ プロバイダー データセンター内の異なるお客様
  - 企業ネットワークの業務またはテスト
  - ロー セキュリティおよびハイ セキュリティの要件
  - 別個の VSAN によるバックアップトラフィック
  - ユーザー トラフィックからのデータの複製
- VSAN は、特定の部門またはアプリケーションのニーズを満たせます。

VSAN の利点

VSAN には、次のような利点があります。

- トラフィックの分離：必要に応じて、トラフィックを VSAN 境界内に含み、1 つの VSAN 内だけに装置を存在させることによって、ユーザー グループ間での絶対的な分離を確保します。
- スケーラビリティ：VSAN は、1 つの物理ファブリック上でオーバーレイされます。複数の論理 VSAN 層を作成することによって、SAN のスケーラビリティが向上します。
- VSAN 単位のファブリック サービス：VSAN 単位のファブリック サービスの複製は、拡張されたスケーラビリティとアベイラビリティを提供します。
- 冗長構成：同一の物理 SAN で作成された複数の VSAN は、冗長構成を保証します。1 つの VSAN に障害が発生した場合、ホストと装置の間にあるバックアップ パスによって、同一の物理 SAN にある別の VSAN に冗長保護が設定されます。
- 設定の容易さ：SANの物理構造を変更することなく、VSAN間でユーザーを追加、移動、または変更できます。ある VSAN から別の VSAN へ装置を移動する場合は、物理的な設定ではなく、ポート レベルの設定だけが必要となります。

最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）です。ユーザー指定の VSAN ID 範囲は 2 ～4093 です。

VSAN の設定

VSAN には、次の属性があります。

- VSAN ID：VSAN ID は、デフォルト VSAN（VSAN 1）、ユーザー定義の VSAN（VSAN 2 ～ 4093）、および独立 VSAN（VSAN 4094）で VSAN を識別します。
- ステート：VSANの管理ステートをactive（デフォルト）またはsuspendedステートに設定できます。VSAN が作成されると、VSAN はさまざまな状態またはステートに置かれます。
  - VSAN の active ステートは、VSAN が設定されイネーブルであることを示します。VSANをイネーブルにすることによって、VSANのサービスをアクティブにします。
  - VSAN の suspended ステートは、VSAN が設定されているがイネーブルではないことを示します。このVSANにポートが設定されている場合、ポートは無効の状態です。このステートを使用して、VSANの設定を失うことなくVSANを非アクティブにします。suspended ステートの VSAN のすべてのポートは、ディセーブルの状態です。VSANをsuspendedステートにすることによって、ファブリック全体のすべてのVSANパラメータを事前設定し、VSAN をただちにアクティブにできます。
- VSAN 名：このテキスト ストリングは、管理目的で VSAN を識別します。名前は、1 ～ 32 文字で指定できます。また、すべての VSAN で一意である必要があります。デフォルトでは、VSAN 名は VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 のデフォルト名は VSAN0003 です。

（注） VSAN 名は一意である必要があります。

- ロードバランシング属性：これらの属性は、ロードバランシングパス選択に対する送信元/送信先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。

（注） 第 1 世代スイッチングモジュールでは、IVR 対応スイッチからの IVR トラフィックに対しては、OX ID ベースのロードバランシングがサポートされませんでした。非 IVR の MDS 9000 シリーズスイッチからの IVR トラフィックの OX ID ベースのロードバランシングは機能します。第 2 世代のスイッチングモジュールでは、IVR 対応スイッチからの IVR トラフィックに対して、OX ID ベースのロードバランシングがサポートされるようになりました。

- ロード バランシング属性は、ロード バランシング パス選択に対する送信元/宛先 ID（src-dst-id）または Originator Exchange ID（OX ID）（デフォルトでは、src-dst-ox-id）の使用を示します。

ポート VSAN メンバーシップ

スイッチのポート VSAN メンバーシップは、ポート単位で割り当てられます。デフォルトでは、各ポートはデフォルト VSAN に属します。2 つの方式のいずれかを使用して、ポートに VSAN メンバーシップを割り当てることができます。

- 静的：VSAN をポートに割り当てる
- 動的：デバイスの WWN に基づいて VSAN を割り当てる

  この方式は、Dynamic Port VSAN Membership（DPVM）と呼ばれます。

VSAN のタイプ

次に、さまざまなタイプの VSAN を示します。

デフォルト VSAN

Cisco MDS 9000 ファミリのスイッチの出荷時の設定値では、デフォルト VSAN 1 だけがイネーブルにされています。VSAN 1 を実稼働環境の VSAN として使用しないことをお勧めします。VSAN が設定されていない場合、ファブリック内のすべてのデバイスはデフォルト VSAN に含まれていると見なされます。デフォルトでは、デフォルト VSAN にすべてのポートが割り当てられています。

（注） VSAN 1 は削除できませんが、中断できます。

最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）です。ユーザー指定の VSAN ID 範囲は 2 ～4093 です。

分離された VSAN

VSAN 4094 は独立 VSAN です。ポートが属する VSAN が削除された場合、非トランキングポートがすべて、この VSAN に転送されます。これにより、デフォルト VSAN または別の設定済みの VSAN へのポートの暗黙的な転送が回避されます。削除された VSAN のポートはすべて、分離されます（ディセーブルされます）。

（注） VSAN 4094 内にポートを設定するか、ポートを VSAN 4094 に移動すると、このポートがすぐに分離されます。

注意 分離された VSAN を使用してポートを設定しないでください。

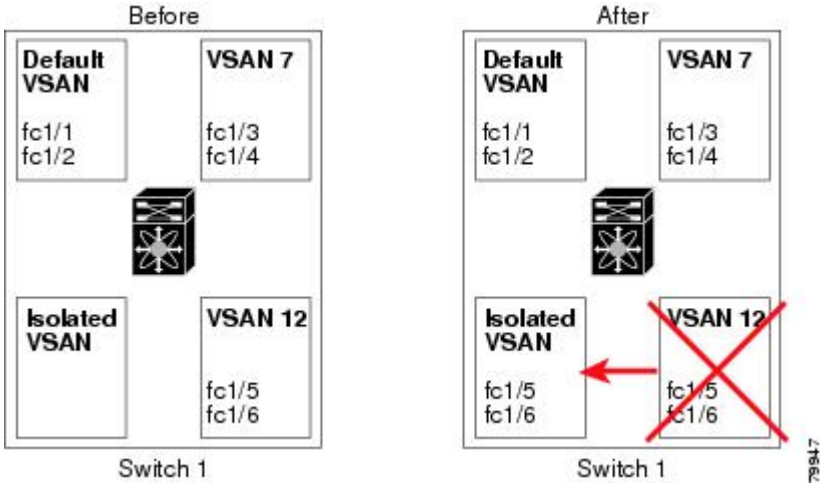
最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）です。ユーザー指定の VSAN ID 範囲は 2 ～4093 です。

スタティック VSAN の削除

アクティブな VSAN が削除されると、その属性が実行コンフィギュレーションからすべて削除されます。VSAN 関連情報は、次のようにシステム ソフトウェアによって保持されます。

- VSAN 属性およびポート メンバーシップの詳細は、VSAN マネージャによって保持されます。コンフィギュレーションから VSAN を削除すると、この機能が影響を受けます。VSAN が削除されると、VSAN 内のすべてのポートが非アクティブになり、ポートが独立 VSAN に移動されます。同一の VSAN が再作成されると、ポートはその VSAN に自動的に割り当てられることはありません。明示的にポート VSAN メンバーシップを再設定します（以下の図を参照）。

図 *10 : VSAN* ポート メンバーシップの詳細



- VSANベースのランタイム（ネームサーバー）、ゾーン分割、および設定（スタティックルート）情報は、VSAN が削除されると削除されます。
- 設定された VSAN インターフェイス情報は、VSAN が削除されると削除されます。

（注） 許可 VSAN リストは、VSAN が削除されても影響を受けません。

設定されていない VSAN のコマンドは拒否されます。たとえば、VSAN 10 がシステムに設定されていない場合、ポートを VSAN 10 に移動するコマンド要求が拒否されます。

VSAN の設定および管理に関する機能情報

次の表に、この機能のライセンス要件を示します。

ライセンスの説明

ENTERPRISE_PKG VSAN を有効にするには、エンタープライズライセンスが必要です。ライセンス方式の詳細については、『Cisco Nexusダッシュボード ファブリック コントローラ Licensing Guide』を参照してください。

ライセンス	ライセンスの説明
ENTERPRISE_PKG	VSAN を有効にするには、エンタープライズライセンスが必要です。ライセンス方式の詳細については、『Cisco Nexusダッシュボード ファブリック コントローラ Licensing Guide』を参照してください。

デフォルトの VSAN 設定

次の表に、設定されたすべての VSAN のデフォルト設定を示します。

パラメータ	デフォルト
デフォルト VSAN	VSAN 1
状態	アクティブ状態
名前	VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。
ロード バランシング属性	OX ID（src-dst-ox-id）

VSAN の作成ウィザード

VSAN 作成ウィザードのワークフローには次のものが含まれます。

- VSAN ID と名前を指定します。
- スイッチを選択します。
- VSAN 属性を指定します。
- VSAN ドメインを指定します。
- VSAN メンバーを指定します。

[仮想管理（Vertial Management）] > [VSANS] を選択します。ドロップダウンリストからファブリックを選択したら、**[新しい VSAN の作成（Create New VSAN）]** アイコンをクリックします。ウィザードのようこそ画面が表示されます。

（注） VSAN がまだ作成されていないことを確認します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用して VSAN を作成して設定するには、次の手順を実行します。

始める前に

VSAN を作成する前には、VSAN に対してアプリケーション特有のパラメータを設定できません。

VSAN がまだ作成されていないことを確認します。中断状態の VSAN を作成しないでください。

（注） 中断状態の VSAN は管理されません。

手順

ステップ 1 [VSAN ID と名前（VSAN ID and Name）] ウィンドウで、次の手順を実行します。

a) ファブリックが [ファブリック（Fabric）] フィールドに対して正しいことを確認します。

b) [VSAN ID] フィールドで、ドロップダウンリストから VSAN ID を選択します。

範囲は 2 ～ 4094 です。ファブリック内の少なくとも 1 つのスイッチで VSAN ID のリストを作成します。VSAN 4079 は予約済み VSAN ID です。

c) [VSAN 名前（VSAN Name）] フィールドに、VSAN の名前を入力します。

（注） このフィールドが空白の場合、スイッチはデフォルトの名前を VSAN に割り当てます。

d) [FICON] チェックボックスをオンにして、スイッチで FICON を有効にします。

e) [次へ（Next）] をクリックします。

ステップ 2 [スイッチの選択（Select Switches）] 画面で、[スイッチ名（Switch Name）] の横にあるチェックボックスをオンにして、VSAN を作成します。

スイッチ名がグレー表示されている場合は、そのスイッチがすでに VSAN の一部であることを示しています。また、前の手順で FICON がオンにされている場合、スイッチで FICON 機能が有効になっていないことを意味する場合もあります。

[次へ（Next）] をクリックします。

ステップ 3 [VSAN 属性の設定（Configure VSAN Attributes）] 画面で、VSAN 属性を設定します。

（注） 中断状態の VSAN を作成した場合、中断状態の VSAN は管理されないため、Cisco Nexusダッシュボード ファブリック コントローラ には表示されません。

a) [ロードバランシング（Load Balancing）] で、VSAN で使用するロードバランシングタイプを選択します。

次のタイプを使用できます。

- Src ID/Dest ID：送信元 ID（Src_ID）と接続先 ID（Dest_ID）のみに基づいています。
- Src ID/Dest ID/Ox ID（デフォルト）：Src_ID および Dest_ID に加えて、発信元交換 ID（Ox_ID）もロードバランシングに使用されます。0x_ID は、ターゲット インターコネクトポートとの交換のために発信元インターコネクトポートによって割り当てられた交換 ID です。

（注） Src ID/Dest ID/0x ID は非 FICON VSAN のデフォルトのロードバランシングタイプであり、FICON VSAN では使用できません。Src ID/Dest ID は FICON VSAN のデフォルトです。

b) [相互運用性（InterOp）] で、相互運用性の値を選択します。

相互運用性の値は、異なるベンダーのデバイスと相互運用するために使用されます。次のいずれかを選択できます。

- デフォルト：相互運用性が無効であることを意味します。
- InterOp-1：VSANがすべてのファイバチャネルベンダーデバイスと相互運用できることを意味します。
- InterOp-2：VSANが基本的な機能から高度な機能まで、特定のファイバチャネル ベンダー デバイスと相互運用できることを意味します。
- InterOp-3：VSANが基本的な機能から高度な機能まで、特定のファイバチャネル ベンダー デバイスと相互運用できることを意味します。
- InterOp-4：VSANが基本的な機能から高度な機能まで、特定のファイバチャネル ベンダー デバイスと相互運用できることを意味します。

（注） 相互運用性は FICON VSAN ではサポートされていません。

c) [管理状態（Admin State）] で、この VSAN の設定可能な状態を選択します。

- アクティブ：VSANが設定され、このVSANのサービスがアクティブであることを意味します。
- 一時停止： VSANは設定されていますが、このVSANのサービスは非アクティブ化されていることを意味します。

  ファブリック全体のすべてのVSANパラメータを事前設定するには、この状態を選択します。

  （注） Nexusダッシュボード ファブリック コントローラ は一時停止された VSAN を管理しないため、VSAN 範囲には表示されません。

d) 順序どおりの配信を許可するには、[順序どおりの配信（InOrder delivery）] チェック ボックスをオンにします。

fcInorderDelivery の値が変更されると、このオブジェクトの値はそのオブジェクトの新しい値に設定されます。

e) FICON VSANのファブリックバインドを有効にする場合は、[ファブリックバインドDBの追加（Add Fabric Binding DB）] 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、選択したスイッチのすべてのピアが、選択したリストの各スイッチに追加されます。

f) FICON VSAN のすべてのポートを禁止する場合は、[すべてのポートを禁止（All Port Prohibited）] チェックボックスをオンにします。

チェックボックスが選択されている場合、FICON VSANは、デフォルトですべてのポートが禁止されているものとして作成されます。

g) [次へ（Next）] をクリックします。

ステップ 4 [VSAN ドメインの設定（Configure VSAN Domain）] 画面で、FICON VSAN の静的ドメイン ID を設定します。

a) [静的ドメイン ID を使用する（Use Static Domain IDs）] チェックボックスをオンにして、VSAN 内のスイッチのドメイン ID を設定します。

b) [使用可能なドメイン ID（Available Domain IDs）] フィールドには、ファブリックで使用可能なすべてのドメイン ID が表示されます。

[使用可能なドメイン ID を自動的に適用（Automatically apply available domain IDs）] をクリックして、VSAN の一部として選択されたすべてのスイッチにドメイン ID を割り当てます。

c) テーブル内のすべてのスイッチについて、使用可能なドメイン ID のリストからドメイン ID を入力します。

d) [次へ（Next）] をクリックします。

ステップ 5 [ポートメンバーシップの設定（Configure Port Membership）] 画面で、VSAN 内のすべてのスイッチについて、インターフェイスを新しい VSAN のメンバーとして設定します。

（注） ポート VSAN を変更すると、インターフェイスの I/O に影響する場合があります。

[次へ（Next）] をクリックします。

ステップ 6 [レビュー（Review）] 画面で、VSAN が正しく設定されているかどうかを確認します。

[前へ（Previous）] をクリックして前の画面に移動し、設定を変更します。

[完了（Finish）] をクリックして確認し、VSAN を設定します。ウィンドウ下部に VSAN の作成結果が表示されます。

（注） VSAN の作成後、新しい VSAN が VSAN 範囲ツリーに表示されるまで数分かかります。

（注） スイッチポートが隔離された VSAN に関連付けられている場合、以前の VSAN 情報は空白になります。

VSLAN の削除

Cisco Nexusダッシュボード ファブリック コントローラ Web UI から VSAN とその属性を削除するには、次の手順を実行します。

手順

ステップ 1 **[仮想管理（Vertial Management）] > [VSANS]** を選択します。

[VSANS] ウィンドウが表示されます。

ステップ 2 [ファブリックの選択] ドロップダウンリストから、VSAN が関連付けられているファブリックを選択します。

選択したファブリックの VSAN スコープツリーが VSANS エリアに表示されます。

ステップ 3 ファブリックを展開し、VSAN の横にある削除アイコンをクリックします。

[VSAN の削除] 画面が表示され、VSAN に関連付けられたスイッチが表示されます。

（注） セグメント化された VSAN は削除できません。

ステップ 4 VSAN を削除するスイッチのチェックボックスを選択します。

[VSANの削除（Delete VSAN）] をクリックします。

確認ウィンドウが表示されます。

ステップ 5 削除を確認する場合は **[確認（Confirm）]** をクリックするか、**[キャンセル（Cancel）]** をクリックして VSAN を削除しないでダイアログボックスを閉じます。

（注） VSAN が削除された後、新しい VSAN が VSAN スコープツリーから消えるまで数分かかります。

VSAN のフィールドと説明

[仮想管理（Virtual Management）] > [VSANS] に表示されるすべてのタブのフィールドと説明は、次の表で説明されています。

[Switches] タブ

このタブには、VSAN スコープのスイッチが表示されます。スイッチ名をクリックして、スイッチの概要情報を表示します。次の表では、[スイッチ]タブに表示されるフィールドについて説明します。

表 *10 : [スイッチ]* タブのフィールドと説明

フィールド	説明
名前	VSAN のスイッチの名前を指定します。 名前をクリックして、スイッチの概要を表示します。 詳細を表示するには、**[詳細の表示（View Details）]** をクリックしてください。
ドメイン ID	永続的なドメイン ID を指定します。
VSAN WWN	VSAN の World Wide Name （WWN）を指定します。

フィールド	説明
プリンシパル WWN	スイッチの World Wide Name （WWN）を指定します。 （注） 主要スイッチの場合、値は *self* です。
モデル	スイッチのモデル名を指定します。
リリース	スイッチの NX-OS バージョンを指定します。
稼働時間	スイッチが起動する時間を指定します。

[ISLs] タブ

このタブには、VSAN スコープ内のスイッチに関する ISL の情報が表示されます。次の表では、ISL タブに表示されるフィールドについて説明します。 VSAN が ISL 全体の両方のスイッチで設定されていて、VSAN が ISL で有効になっていない場合、Nexusダッシュボード ファブリック コントローラ では、VSAN はセグメント化されていると見なされます。したがって、VSAN を ISL 全体のトランク VSAN に追加して、警告メッセージをクリアします。または、この警告メッセージを無視することもできます。

表 *11 : [ISL]* タブのフィールドと説明

フィールド	説明
VSAN	この ISL がトラフィックを実行するすべての VSAN。
スイッチから	リンクのソーススイッチ。
送信元インターフェイス	リンクのソース E_port のポートインデックス。
スイッチに	リンクのもう一方の端にあるスイッチ。
インターフェイスへ	リンクの宛先 E_port のポートインデックス。
スピード	この ISL の速度。
ステータス	リンクの動作ステータス。
ポートチャネルメンバー	ISL がポートチャネルの場合は、ポートチャネルのメンバー。
追加情報	TE/TF/TNP ISL など、この ISL に関する追加情報。

[ホストポート] タブ

このタブには、VSAN スコープ内のスイッチのホストポートに関する情報が表示されます。次の表では、[ホストポート] タブに表示されるフィールドについて説明します。

表 *12 : [*ホストポート*]* タブのフィールドと説明

フィールド	説明
エンクロージャ	エンクロージャの名前
デバイス エイリアス	このエントリのデバイスエイリアス。
ポートWWN	このホストに割り当てられた PWWN。
Fcid	このホストに割り当てられた FC ID。
スイッチ インターフェイス	エンドデバイスに接続されているスイッチのインターフェイス。
リンクステータス	リンクの動作ステータス。
ベンダー	ベンダーの名前を指定します。
シリアル番号（Serial Number）	エンクロージャのシリアル番号を指定します。
モデル	モデルの名前を指定します。
ファームウェア	このHBAによって実行されるファームウェアのバージョン。
要因	この HBA によって実行されるドライバのバージョン。
追加情報	この HBA に対応する情報一覧です。

[ストレージポート] タブ

このタブには、VSAN スコープ内のスイッチのストレージポートに関する情報が表示されます。次の表では、[ストレージポート] タブに表示されるフィールドについて説明します。

表 *13 : [*ストレージポート*]* タブのフィールドと説明

フィールド	説明
エンクロージャ	エンクロージャの名前
デバイス エイリアス	このエントリのデバイスエイリアス。
ポートWWN	このホストに割り当てられた PWWN。
Fcid	このホストに割り当てられた FC ID。
スイッチ インターフェイス	エンドデバイスに接続されているスイッチのインターフェイス。
リンクステータス	リンクの動作ステータス。

[属性（Attributes）] タブ

このタブには、VSANスコープ内のすべてのスイッチの属性が表示されます。次の表では、[属性] タブに表示されるフィールドについて説明します。

表 *14 : [*属性*]* タブのフィールドと説明

フィールド	説明
編集	**[**編集（**Edit**）**]** をクリックして、VSAN の属性を変更し、同じ VSAN 属性を選択したスイッチにプッシュします。 選択したいずれかのスイッチで VSAN が FICON VSAN の場合、次のフィールドは FICON VSAN では変更できないため、UI に表示されません。 • vsanLoadBalancing • 相互運用性 • 順序どおりの配信 属性を変更したら、**[**保存（**Save**）**]** をクリックして変更を保存するか、**[**キャンセル（**Cancel**）**]** をクリックして破棄します。
スイッチ名	VSAN に関連付けられているスイッチの名前を表示します。
VSAN 名	VSAN の名前を表示します。
Admin	Admin の状態がアクティブであるか一時停止であるかを指定します。 • **[**アクティブ（**Active**）**]** は、VSAN が設定され、VSAN のサービスがアクティブ化されていることを意味します。 • **[**ダウン（**Down**）**]** は、VSAN が設定されていることを意味します。ただし、VSAN のサービスは非アクティブ化されています。set this state を使用すると、CLI のみを使用して、すべての VSAN パラメータを事前設定できます。 （注） VSAN を一時停止すると、Cisco Nexus ダッシュボード ファブリック コントローラ からも削除されます。
Oper	VSAN の動作状態。
MTU	スイッチの MTU を表示します。

フィールド	説明
ロード バランシング	VSAN で使用されるロードバランシングタイプを指定します。 VSAN で使用されるロードバランシングの種類です。 • srcId/DestId — パス選択にソース ID と接続先 ID を使用 • srcdId/DestId/Oxld — ソース、接続先、交換 ID を使用
相互運用性	この VSAN のローカルスイッチの相互運用モード。 • デフォルト • 相互運用性 - 1 • 相互運用性 - 2 • 相互運用性 - 3
順序どおりの配信	デバイスの順序どおりの配信保証フラグ。true の場合、順序どおりの配信が保証されます。false の場合、保証されません。
FICON	VSAN が FICON 対応の場合は true。

[ドメイン ID] タブ

このタブには、VSAN ドメインとそのパラメータに関する情報が表示されます。次の表では、ドメイン ID タブのフィールドについて説明します。

表 *15 : [*ドメイン *ID]* タブのフィールドと説明

フィールド	説明
編集	スイッチを選択し、[編集] アイコンをクリックして、選択したスイッチのドメイン ID 情報を変更します。
スイッチ名	VSAN のスイッチ名を指定します。 （注） NPV スイッチは、この列には表示されません。ただし、NPV スイッチはこの VSAN ファブリックに存在します。
状態	スイッチのステータスを指定します。
有効	ドメイン ID を有効にするか無効にするかを指定します。
Running	実行中のドメインを指定します。
設定	設定を指定します。

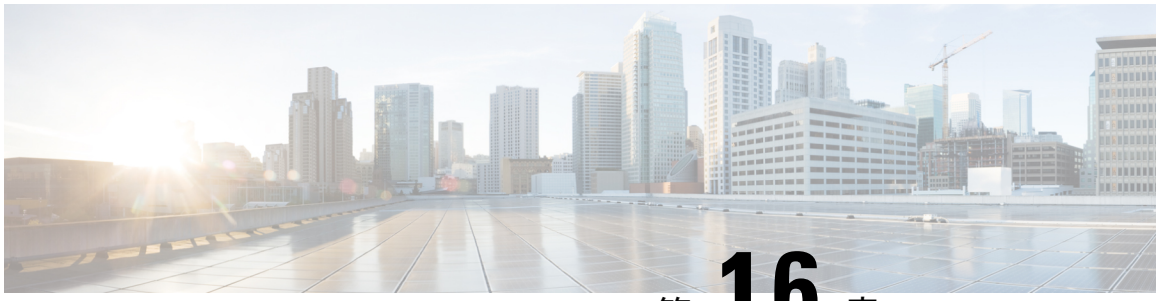
フィールド	説明
設定タイプ	ドメイン ID タイプの使用方法を **[優先（preferred）]** または **[静的（static）]** に指定します。
アイコン	
Total	テーブルの隣の番号は、このタブの下のエントリを指定します。
更新アイコン	更新アイコンをクリックしてエントリを更新します。

[VSAN メンバーシップ] タブ

このタブには、VSANを形成するスイッチのインターフェイスに関する情報が表示されます。次の表では、[VSAN メンバーシップ] タブのフィールドについて説明します。

表 *16 : [VSAN* メンバーシップ*]* タブのフィールドと説明

フィールド	説明
編集	スイッチを選択し、[編集] アイコンをクリックして、選択したVSANおよび選択したスイッチのポート VSAN メンバーシップを変更します。 ポート VSAN メンバーシップは、FC (物理)、ポートチャネル、FCIP、iSCSI、VFC (スロット/ポート)、VFC (ID)、VFC チャネル、VFC FEX、および VFC ブレイクアウトを含むさまざまなタイプによって提供されます。PortChooserは、選択したスイッチに存在するすべてのインターフェイスを表示し、ユーザーが選択できるようにタイプごとに提供されます。 （注） 動作中のトランキングポートまたはポートチャネルメンバーのポスト VSAN メンバーシップを変更すると、警告が表示されます。デバイスマネージャを使用して、トランキングインターフェイスの許可 VSAN リストを変更します。
スイッチ名	スイッチの名前
インターフェイス	VSAN の FC ポート



第 16 章

仮想インフラストラクチャ マネージャ

仮想インフラストラクチャ マネージャ

UI パス：**[仮想管理（Virtual Management）]** > **[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]**

（注） Cisco Nexus Dashboard ファブリックコントローラの仮想マシンのネットワーク可視化機能が有効になっていることを確認します。

1. **[設定（Settings）]** > **[機能管理（Feature Management）]** を選択し、次のチェックボックスをオンにします。
   - Kubernetes ビジュアライザ
   - VMM ビジュアライザ
   - OpenStack ビジュアライザ
2. [Apply] をクリックします。

次の表では、[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）] ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
[サーバ（Server）]	サーバー IP アドレスを指定します。

フィールド	説明
タイプ	次のいずれかのインスタンスのタイプを指定します。 • vCenter • Kubernetesクラスタ • OpenStack クラスタ
管理対象（Managed）	管理対象または管理対象外のクラスタのステータスを指定します。
ステータス	追加されたクラスタの状態を指定します。
ユーザー（User）	クラスタを作成したユーザーを指定します。
最終更新時刻	クラスタの最終更新時刻を指定します。

（注） **[更新（Refresh）]** アイコンをクリックして、仮想インフラストラクチャ マネージャ テーブルを更新します。

次の表では、[アクション（Actions）] メニューのドロップダウン リストで、[仮想インフラストラクチャ マネージャ（Virtual Infrastracture Manager）] に表示されるアクション項目について説明します。

アクション項目	説明
インスタンスの追加	**[アクション（Actions）]** ドロップダウンリストから **[インスタンスの追加（Add Instance）]** を選択します。詳細については、「インスタンスの追加」を参照してください。 （注） ルート上で同じ IP アドレスを設定していることを確認します。「ルート IP アドレスの設定」を参照してください。
インスタンスの編集	編集するインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから **[インスタンスの編集（Edit Instance）]** を選択します。必要な変更を行って、**[保存（Save）]** をクリックします。**[キャンセル（Cancel）]** をクリックして、変更を破棄します。
インスタンスの削除	削除する1つ以上の必要なインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[削除（Delete）]** を選択します。[確認（Confirm）] をクリックしてインスタンスを削除します。**[キャンセル（Cancel）]** をクリックしてこの削除を破棄します。

アクション項目	説明
インスタンスの再検出	再検出する1つ以上の必要なインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[インスタンスの再検出（Rediscover Instance(s)）]** を選択します。確認メッセージが表示されます。

詳細については、次を参照してください。

Cisco UCS B シリーズ ブレードサーバーのサポート

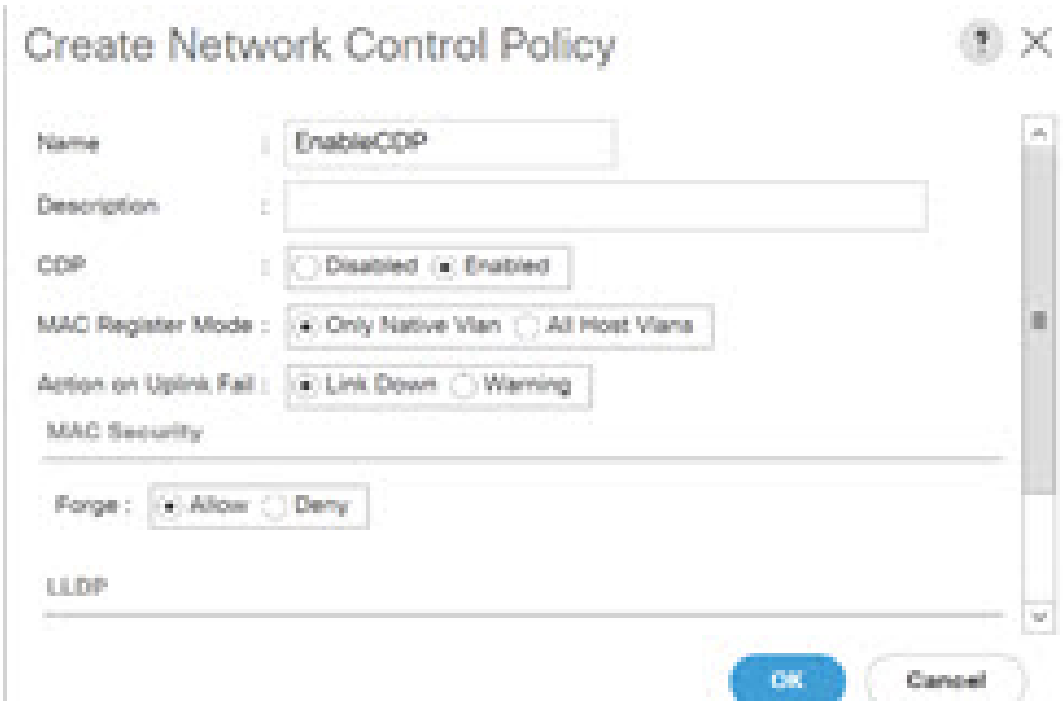
NDFC は、ファブリックインターコネクトの背後にある UCS タイプ B （シャーシ UCS）で実行されているホストをサポートします。この機能を使用するには、Cisco UCSM で vNIC の CDP を有効にする必要があります。

（注） デフォルトでは、CDP は Cisco UCSM で無効になっています。

参考のために、VMM-A と VMM-B の 2 つの VMM について考えてみましょう。Cisco UCS UCS B シリーズ ブレードサーバーの検出後、トポロジに青色の VMM-A と VMM-B がファブリック インターコネクト ノードであることが表示されます。トポロジの例を下図に示します。

UCSM で CDP を有効にするには、次の手順を使用して新しいネットワーク制御ポリシーを作成する必要があります。

1. USCM で、**[LAN]** を選択し、ポリシーを展開します。
2. **[ネットワーク制御ポリシー（Network Control Policies）]** を右クリックして、新しいポリシーを作成します。
3. [名前（Name）] フィールド、にポリシーの名前を **EnableCDP** と入力します。
4. CDP の**有効な**オプションを選択します。



5. **[OK]** をクリックしてポリシーを作成します。

新しいポリシーを ESX NIC に適用するには、次の手順を実行します。

- 更新された vNIC テンプレートを使用している場合は、ESXi vNIC の各 vNIC テンプレートを選択し、[ネットワーク制御ポリシー] ドロップダウンリストから EnableCDP ポリシーを適用します。
- vNIC テンプレートを使用していない場合は、更新されたサービス プロファイル テンプレートを使用します。各サービス プロファイル テンプレートに EnableCDP ポリシーを適用します。
- 1 回限りのサービスプロファイルを使用している場合（つまり、各サーバーが独自のサービスプロファイルを使用している場合）、すべてのサービスプロファイルに移動し、すべての vNIC で EnableCDP ポリシーを有効にする必要があります。

Cisco UCSM の詳細については、『Cisco UCSM ネットワーク管理ガイド』を参照してください。

ルート IP アドレスの設定

IP アドレスを vCenter に追加する前に、Cisco Nexus ダッシュボードで同じ IP アドレスを設定する必要があります。

Cisco Nexus ダッシュボードでルートを設定するには、次の手順を実行します。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[クラスタ設定（Cluster Configuration）]** を選択します。

ステップ 2 **[全般（General）]** タブの **[ルート（Routes）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[ルート（Routes）] ウィンドウが表示されます。

ステップ 3 IP アドレスを設定するには、**[管理ネットワーク ルートの追加（Add Management Network Routes）]** をクリックし、必要な IP アドレスを入力して、**[チェック（check）]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

ルート設定は、次の 2 つのシナリオによって管理されます。

1. アプリケーションサーバーである vCenter の場合、通常は管理ネットワーク経由で到達可能です。
2. vCenter によって管理される ESXi サーバーと、K8s インスタンスや OpenStack インスタンスをホストするベアメタルサーバーは、ファブリックネットワークに直接接続されます。したがって、それらはデータネットワークを介して到達可能です。

vCenter の可視化の追加

[仮想的な管理（Virtual Management）] > **[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]** に表示される **[アクション（Actions）]** メニューのドロップダウンリストで、さまざまなアクションを実行できます。

手順

ステップ 1 **[アクション（Actions）]** **[インスタンスの追加（Add Instance）]** を選択します。

[インスタンスの追加（Add Instance）] ウィンドウが表示されます。

ステップ 2 [タイプの選択（Select Type）]ドロップダウン リストから **[vCenter]** を選択します。

必要な IP アドレスまたはドメイン名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [Add] をクリックします。

追加された vCenter クラスタは、**[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]** ウィンドウで表示できます。

ステップ 4 インスタンスを編集するには、必要な vCenter を選択して、**[アクション（Actions）]>[インスタンスの編集（Edit Instance）]** を選択して、**[保存（Save）]** をクリックします。

選択済みの vCenter クラスタのパスワードをアップデートし、ステータスを「管理対象」または「管理対象外」に変更できます。

（注） 管理対象外ステータスの vCenter クラスタの場合、ダッシュボードでトポロジと vCenter クラスタの詳細を表示できません。

ステップ 5 1 つ以上の vCenter クラスタを削除するには、必要な vCenter を選択し、**[アクション（Actions）] > [インスタンスの削除（Delete Instance(s)）]** を選択して、**[変更の確認（Confirm changes）]** をクリックします。

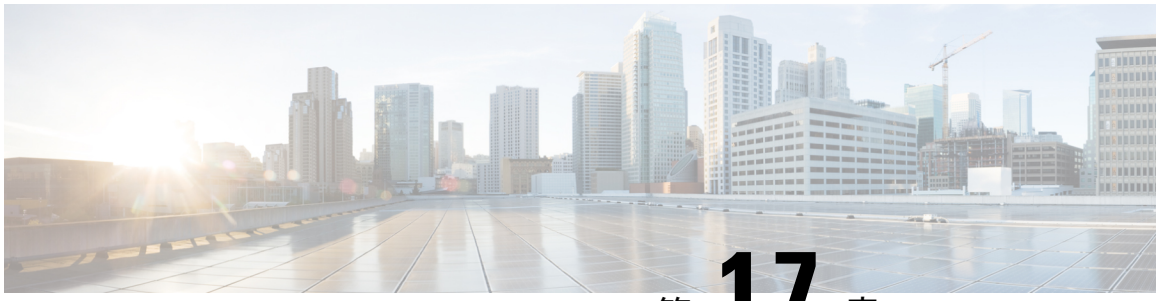
（注） クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。

ステップ 6 1 つ以上の vCenter クラスタを再検出するには、必要な vCenter を選択して、**[アクション（Actions）] > [インスタンスの再検出（Rediscover Instance(s)）]** を選択します。

確認メッセージが表示されます。

第 III 部

設定



第 17 章

サーバ設定

サーバ設定

デフォルト値として入力されるパラメータを設定できます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI から Nexusダッシュボード ファブリック コントローラ サーバのパラメータを設定するには、次の手順を実行します。

1. **[設定（Settings）] > [サーバ設定（Server Settings）]** を選択します。

   サーバ設定はさまざまなタブに分類され、

2. 要件に基づいて設定を変更します。

3. **[保存（Save）]** をクリックして設定を適用します。

Admin 下での LAN デバイス管理の接続性

この設定は、Nexus ダッシュボード ファブリック コントローラに必要な POD の永続的な IP の使用を決定します。ユーザーが初めてファブリック コントローラ ペルソナを選択すると、永続的な IP が Nexus ダッシュボードに割り当てられているかどうかを確認するための事前チェックが行われます。永続的な IP が割り当てられていない場合、オペレーターはエラーを表示します。ユーザーは、Nexus Dashboard 管理ネットワークまたは Nexus Dashboard データネットワークのいずれかで永続的な IP を提供できます。この選択に基づいて、ユーザーは、NDFC アプリケーションページのサーバー設定の下にある LAN デバイス管理の接続性の下でオプションを指定する必要があります。デフォルトでは、[管理] が選択されていますが、ユーザーが Nexus ダッシュボードデータ ネットワークで永続的な IP を提供する場合、ユーザーはオプションとして [データ] を選択する必要があります。

SMTP 下の SMTP ホスト

この設定は、プログラム可能なレポートとアラームの EMAIL アウトオブバンド通知として使用されます。NDFC 12.0.1a リリース以降、ユーザーは電子メール通知で NDFC アラームとレポートを受信できるようになりました。SMTP ホスト アドレスは、Nexus ダッシュボード管理

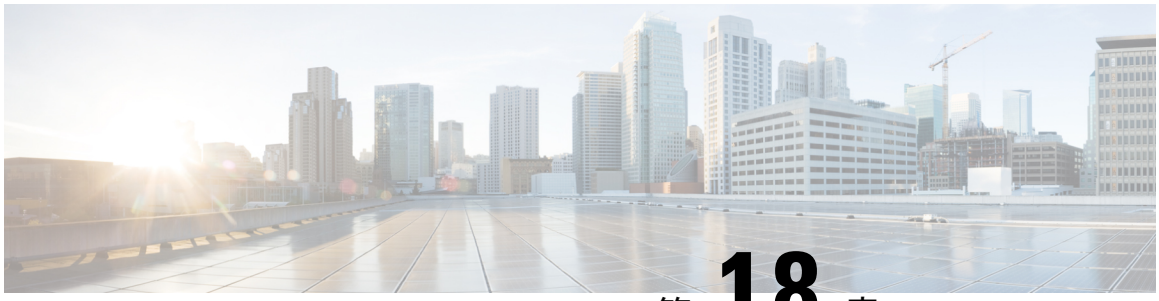
インターフェイスを介して到達可能である必要があります。Nexus ダッシュボード管理インターフェイスとSMTPホストが異なるIPサブネットの一部である場合、ユーザーはNexusダッシュボードクラスタ構成で静的ルートエントリを作成する必要があります。

LAN ファブリックの下のすべてのファブリックで展開を無効にする

この設定により、NDFCインスタンスで定義されているすべてのファブリックの展開が無効になります。ユーザーは、ファブリックレベルごとに展開を有効にすることはできません。たとえば、ユーザーが3つのファブリックを持っている場合、構成の観点から3つのファブリックすべてが無効になります。ユーザーは、必要に応じてさまざまな構成のステージングを続けることができます。後で、ユーザーは、このサーバー設定のチェックを外すことにより、展開アクションを有効にすることができます。

PM 下の LAN スイッチの温度を収集する

この設定により、スイッチの温度の詳細を収集し、それを [ファブリックの概要] と [メトリック] セクションに表示することができます。デフォルトでは、温度データは収集されません。この設定を有効にすると、ユーザーはファブリックスイッチの温度情報も表示できます。



第 18 章

Feature Manager

Feature Manager

Cisco DCNM リリース 11.x では、DCNM のインストール時にインストール モードを選択する必要があります。リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ では Nexus Dashboard にサービスをインストールできます。Nexusダッシュボード ファブリック コントローラ UI を起動すると、[機能管理（Feature Management）] ページに 3 つの異なるインストールモードが表示されます。

Nexusダッシュボード ファブリック コントローラ 12では、機能セットを動的に有効にし、アプリケーションを拡張できます。**[設定（Settings）] > [機能管理（Feature Management）]** の順に選択して、インストーラ タイプを選択し、選択した展開でいくつかの機能を有効または無効にします。

Cisco Nexus Dashboard から Nexusダッシュボード ファブリック コントローラ を初めて起動すると、[機能管理（Feature Management）]画面が表示されます。機能セットを選択する前に、バックアップと復元の操作のみを実行できます。

[機能管理（Feature Management）] ページで、次のインストール モードのいずれかを選択できます。

- ファブリック検出
- ファブリック コントローラ
- SAN コントローラ

機能セットを選択した後、Nexus Dashboard から Cisco Nexusダッシュボード ファブリック コントローラ を起動すると、次のログインから Dashboard ページが開きます。

フィーチャ セットの選択

Cisco Nexusダッシュボード ファブリック コントローラ 12を初めて起動すると、どのフィーチャ セットも有効になりません。この状態で、バックアップと復元を実行して、DCNM 11.5(x)

データをNexusダッシュボードファブリック コントローラ12に復元できます。Nexusダッシュボード ファブリック コントローラはバックアップ ファイルからデータを読み取り、それに応じてインストーラ タイプを選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からフィーチャ セットを展開するには、次の手順を実行します。

手順

ステップ 1 **[設定（Settings）] > [機能管理（Feature Management）]** を選択します。

ステップ 2 ペルソナを選択して、デフォルトの機能セットを表示します。

Cisco NDFC ペルソナで使用できる機能については、「各ペルソナの機能 （200 ページ）」を参照してください。

ステップ 3 次の表で、機能セットで使用可能な機能名に対してチェックボックスをオンにします。

ステップ 4 [Apply] をクリックします。

フィーチャ セットが展開されます。選択したアプリケーションが有効になります。フィーチャ セットがインストールされていることを示すメッセージが表示されます。有効にするには更新する必要があります。

ステップ 5 ブラウザを更新して、選択したフィーチャ セットとアプリケーションでNexusダッシュボード ファブリック コントローラ を展開します。

左側のペインには、展開されたフィーチャ セットで特にサポートされている機能が表示されます。

各ペルソナの機能

次の表に、Cisco NDFC リリース 12.1.1e で使用可能な機能に関する情報を示します。

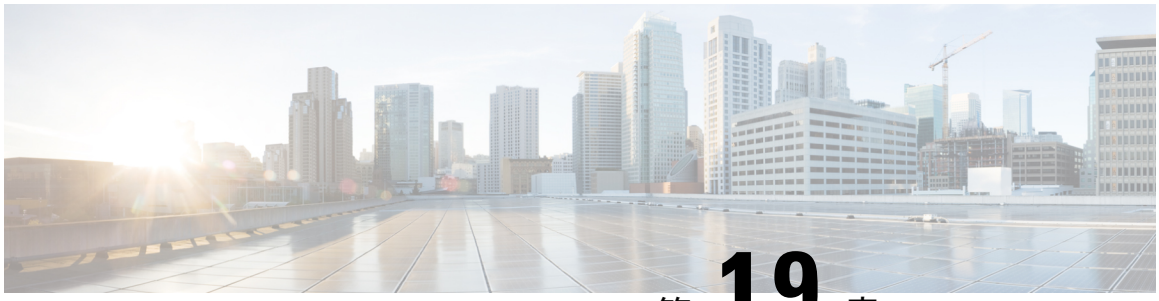
機能セット全体での変更

Nexusダッシュボード ファブリック コントローラ 12では、ある機能セットから別の機能セットに切り替えることができます。**[設定（Settings）] > [機能管理（Feature Management）]** を選択します。次の表で、目的の機能セットとアプリケーションを選択します。[保存して続行（Save and Continue）] をクリックします。ブラウザを更新して、新しい機能セットとアプリケーションでシスコ Nexusダッシュボード ファブリック コントローラ の使用を開始します。

特定の展開でサポートされる機能/アプリケーションがいくつかあります。機能セットを変更すると、これらの機能の一部は新しい展開でサポートされません。次の表に、機能セットを変更できる前提条件と基準の詳細を示します。

表 *17 :* 展開間でサポートされるスイッチング

送信元/宛先	ファブリック検出	ファブリック コントローラ	SAN コントローラ
ファブリック検出	-	ファブリック検出の展開では、モニタモードファブリックのみがサポートされます。機能セットを変更すると、ファブリック コントローラ導入でファブリックを使用できます。	サポート対象外
ファブリック コントローラ	ファブリックセットを変更する前に、既存のファブリックを削除する必要があります。	Easy Fabric から IPFM ファブリック アプリケーションに変更する場合は、既存のファブリックを削除する必要があります。	サポート対象外
SAN コントローラ	サポート対象外	サポート対象外	-



第 19 章

クレデンシャル管理

SAN クレデンシャル管理

[設定（Settings）] [SAN クレデンシャル管理（SAN Credentials Management）] を選択して、ファブリック シードスイッチへのSNMPアクセスの詳細を表示します。ユーザがすべてのファブリックへのアクセスを検証した場合は、ファブリックのすべてのシード スイッチの SNMP クレデンシャルが表示されます。

Cisco Nexusダッシュボード ファブリック コントローラのスイッチク レデンシャル ウィンドウには、次のフィールドがあります。

フィールド	説明
シード スイッチ	スイッチの IP アドレス。
ユーザ名	Cisco Nexusダッシュボード ファブリック コントローラのユーザのユーザ名を指定します。
[パスワード（Password）]	スイッチ SNMP ユーザの暗号化形式を表示します。
SNMPv3 / SSH	SNMP プロトコルが検証されるかどうかを指定します。 デフォルト値は **false** です。
認証/プライバシー	認証プロトコルを指定します。 デフォルト値は **[NOT_SET]** です。
ステータス	スイッチのステータスを表示します。

Cisco Nexusダッシュボード ファブリック コントローラユーザが SNMP を使用してファブリックを設定する前に、ユーザはファブリックのシード スイッチに SNMP クレデンシャルを提供

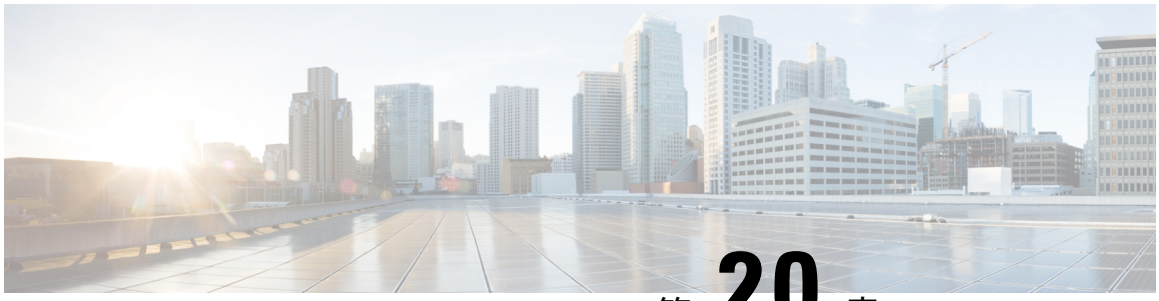
し、検証する必要があります。ユーザがファブリック シード スイッチの有効なクレデンシャルを提供しない場合、[スイッチ クレデンシャル（Switch Credentials）] テーブルに SNMPv3/SSH および AuthPrivacy フィールドのデフォルト値が表示されます。

次の表では、**[アクション（Actions）]** メニューのドロップダウン リストで、**[設定（Settings）] > [SAN クレデンシャル管理（SAN Credentials Management）]** に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルから行を選択し、**[編集（Edit）]** を選択してスイッチ クレデンシャル情報を更新します。
クリア（Clear）	スイッチ クレデンシャルをクリアします。
検証	スイッチ クレデンシャルを再検証します。

第 IV 部

操作



第 20 章

イベント分析

ここでは、次の内容について説明します。

アラーム

このタブには、さまざまなカテゴリに対して生成されたアラームが表示されます。このタブには、ID（オプション）、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、最終更新日（オプション）、ポリシー、メッセージなどの情報が表示されます。このタブで [更新間隔（Refresh Interval）] を指定できます。1 つ以上のアラームを選択し、[ステータスの変更（Change Status）] ドロップダウンリストを使用して、アラームのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。

発行されたアラーム

UI パス：**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）]** の順に選択します。

1. 新しいアラーム ポリシーを作成した後、**[発生したアラーム（Alarms Raised）]** タブに移動し、**[更新（Refresh）]** アイコンをクリックして、作成したアラームを表示します。

   新しく作成されたアラームが表示されます。

2. [アラーム（Alarms）] テーブルの **[重大度（Severity）]** をクリックすると、同じ ITL/ITN フローで同じポリシーによって発生したアラームの履歴が表示されます。

3. **[ポリシー（Policy）]** 列の [ポリシー名（Policy name）] をクリックして、チャートを表示します。

   スライドイン ペインが表示され、内部にグラフが表示されます。

4. グラフを表示するには、ドロップダウン リストから必要な**メトリック**を選択します。

（注） これらのメトリックは、SAN Insights Anomaly Policy でのみ表示できます。

次の表では、**[操作（Operations）]>[イベント分析（Event Analytics）]>[アラーム（Alarms）]>[発生したアラーム（Alarms Raised）]** に表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元の名前を指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
ポリシー	アラームのポリシーを指定します。
Message	メッセージを表示します。
Ack User	アラームを確認したユーザのユーザ名。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
確認応答あり	1つまたは複数のアラームを選択し、**確認**を選択します。アラームをブックマークし、**[確認済み（Acknowledged）]** の列にAck User 名を追加できます。
未確認	1 つまたは複数のアラームを選択し、**未確認**を選択して、ブックマークされたアラームを削除します。 （注） 確認済みアラームのみを未確認にすることができます。
クリア	アラームを選択し、**消去**を選択して、アラームポリシーを手動で消去します。 消去されたアラームは、**[消去されたアラーム（Alarm Cleared）]** タブに移動します。
アラームの削除	アラームを選択し、**削除**を選択してアラームを削除します。

クリアされたアラーム

UI パス：**操作 > イベント分析 > アラーム > クリアされたアラーム**

[クリアされたアラーム（Alarms Cleared）] タブには、**[発行されたアラーム（Alarms Raised）]** タブでクリアされたアラームのリストがあります。このタブには、ID（オプション）、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、クリア時（オプション）、クリア

元、ポリシー、メッセージなどの情報が表示されます。最大 90 日間、クリアされたアラームの詳細を表示できます。

1 つ以上のアラームを選択し、**[アクション（Actions）] > [削除（Delete）]** をクリックしてそれらを削除できます。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元アラーム IP アドレスを指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
クリアされた時間	アラームがクリアされた時刻を指定します。
クリアしたユーザ	アラームをクリアしたユーザを指定します。
ポリシー	アラームのポリシーを指定します。
Message	アラームの CPU 使用率およびその他の詳細を指定します。
Ack User	確認応答されたユーザ ロール名を指定します。

次の表では、**[発行されたアラーム（Alarms Raised）]** タブに表示される **[アクション（Actions）]** メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
アラームの削除	アラームを選択し、**[削除（Delete）]** を選択して、クリアされたアラームを削除します。

アラーム ポリシーの監視と追加

SAN コントローラでアラームを有効にし、**[操作（Operations）]**>**[イベント分析（Analytics）]**> **[アラーム（Alarms）]**に移動し、垂直タブの **[アラーム ポリシー（Alarm Policies）]** をクリックします。[外部アラームの有効化]チェックボックスが選択されていることを確認します。これを有効にするには、 SAN Controller Server を再起動する必要があります。

SAN コントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SAN コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、**[外部アラームの有効化（Enable external alarms）]** チェックボックスがオンになっていることを確認します。これを有効にするには、 SAN Controller Server を再起動する必要があります。

SAN コントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SAN コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、alarm.trap.listener.address フィールドに外部ポート アドレスを入力し、**[変更の適用（Apply Changes）]** をクリックして、SAN コントローラを再起動します。

（注） **[アラーム ポリシーの作成（Alarm Policy creation）]** ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** に表示されるフィールドについて説明します。

フィールド	説明
名前	アラーム ポリシーの名前を指定します
説明	アラーム ポリシーの名前を指定します
ステータス	アラーム ポリシーのステータスを指定します。 • アクティブ • 非アクティブ
ポリシータイプ	ポリシーのタイプを指定します。 • デバイスのヘルス ポリシー • インターフェイスのヘルス ポリシー • syslog アラームポリシー • SAN Insights の異常ポリシー
Devices	アラーム ポリシーを適用するデバイスを指定します。
インターフェイス	インターフェイスを指定します。
詳細	ポリシーの詳細を指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストのアクション項目について説明します。この項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** に表示されます。

アクション項目	説明
新しいアラーム ポリシーの作成	新しいアラーム ポリシーを作成することを選択します。「新しいアラーム ポリシーの作成」の項を参照してください。
編集	アラーム ポリシーを編集するには、ポリシーを選択し、**[編集（Edit）]**を選択します。

アクション項目	説明
削除	アラーム ポリシーを削除するには、ポリシーを選択し、**[削除（Delete）]** を選択します。
アクティブ化（Activate）	アラーム ポリシーをアクティブ化して適用するには、ポリシーを選択し、**[アクティブ化（Activate）]**を選択します。
非アクティブ化	アラーム ポリシーを無効にして非アクティブにするには、ポリシーを選択し、**[非アクティブ化（Deactivate）]** を選択します。
インポート	.csv ファイルからアラーム ポリシーを一括でインポートする場合に選択します。
エクスポート	アラーム ポリシーを .csv ファイルから一括でエクスポートする場合に選択します。

次のアラーム ポリシーを追加できます。

- **デバイス ヘルス ポリシー**：デバイス ヘルス ポリシーを使用すると、デバイス ICMP到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。
- **インターフェイス ヘルス ポリシー**：インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。
- **Syslog アラーム ポリシー**：Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。
- **San Insights Anomaly Policy**：San Insights Anomaly Policy では、SAN Insight データを使用して、ファブリック内の問題を特定するためのカスタマイズされたアラームを作成できます。

新しいアラーム ポリシーの作成

次のアラーム ポリシーを追加できます。

- デバイスのヘルス ポリシー
- インターフェイスのヘルス ポリシー
- syslog アラームポリシー
- SAN Insights の異常ポリシー

デバイスのヘルス ポリシー

デバイスヘルスポリシーを使用すると、デバイス ICMP 到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。

ポリシーを作成するデバイスを選択します。ポリシー名、説明、CPU使用率パラメータ、メモリ使用率パラメータ、環境温度パラメータ、デバイスの可用性、およびデバイス機能を指定します。**[デバイス機能（Device Features）]** で、BFD、BGP、および HSRP プロトコルを選択できます。これらのチェックボックスをオンにすると、**BFD**-ciscoBfdSessDown、ciscoBfdSessUp、**BFD**-bgpEstablishedNotification、bgpBackwardTransNotification、cbgpPeer2BackwardTransition（）、cbgpPeer2EstablishedNotification、および **HSRP**-cHsrpStateChange のアラームがトリガーされます。トラップ OID 定義の詳細については、「https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do」を参照してください。

インターフェイスのヘルス ポリシー

インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMPリスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。 SAN コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。SMTPパラメータを設定し、**[保存（Save）]** をクリックして、SAN コントローラ サービスを再起動します。
- リンクステート：リンクステートオプションを選択して、インターフェイスリンクのアップまたはダウンを確認します。リンクダウンの場合、アラームを発生させることができ、リンクアップでアラームをクリアできます。
- 帯域幅（イン/アウト）：
- インバウンドエラー

- アウトバウンドエラー
- インバウンド破棄
- アウトバウンド破棄

Syslog アラーム

Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- デバイス：このポリシーの範囲を定義します。このポリシーを適用する個々のデバイスまたはすべてのデバイスを選択します。
- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMP リスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで**[転送（Forwarding）]**チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。 SAN コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。 SMTPパラメータを設定し、**[保存（Save）]** をクリックして、SAN コントローラ サービスを再起動します。
- 重大度：この syslog アラーム ポリシーの重大度レベルを定義します。選択肢は、Critical、Major、Minor、および Warning です。
- 識別子：発生およびクリア メッセージの識別子部分を指定します。
- Raise Regex：syslog 発生メッセージの形式を定義します。構文は次のとおりです。 Facility-Severity-Type：メッセージ
- Clear Regex：syslog クリア メッセージの形式を定義します。構文は次のとおりです。 Facility-Severity-Type：メッセージ

正規表現の定義は単純な式ですが、完全な正規表現ではありません。テキストの可変領域は、$(LABEL) 構文を使用して示されます。各ラベルは、1 つ以上の文字に対応する正規表現キャプチャ グループ（.+）を表します。2 つのメッセージを関連付けるために、raise メッセージと clear メッセージの両方にある可変テキストが使用されます。識別子は、両方のメッセージに表

示される1つ以上のラベルのシーケンスです。識別子は、ckear syslogメッセージをアラームを発生させたsyslogメッセージと照合するために使用されます。テキストがメッセージの1つだけに表示される場合は、ラベルを付けて識別子から除外できます。

例：「値」が「ID1-ID2」のポリシー

```
"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."
```

この例では、ID1 および ID2 ラベルをアラームとして検出するための識別子としてマークできます。この識別子は、対応するsyslogメッセージで見つかります。ラベル「REASON」は昇格ですが、クリアメッセージにはありません。このラベルは、アラームをクリアするsyslogメッセージに影響しないため、識別子から除外できます。

表 *18* : 例 *1*

識別子	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_ADMIN_UP：インターフェイス Ethernet15/1 で admin が起動されています。
正規表現のクリア	ETHPORT-5-IF_DOWN_NONE：インターフェイス Ethernet15/1 がダウンしています（トランシーバ欠落）

上記の例では、正規表現は端末モニタに表示される syslog メッセージの一部です。

表 *19* : 例 *2*

Identifier	ID1-ID2
正規表現を上げる	ETH_PORT_CHANNEL-5-PORT_DOWN：$（ID1）：$（ID2）がダウンしています
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP：$（ID1）：$（ID2）が起動しています

表 *20* : 例 *3* :

Identifier	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning clear

エンドポイント ロケータ アラーム

アラームは、エンドポイントロケータ（EPL）によって外部アラームカテゴリに登録および作成されます。

アラームポリシー

EPL 外部アラームカテゴリポリシーは、ファブリックで EPL が有効になっているときにアクティブになります。アラームは、重複する IP アドレス、重複する MAC アドレス、VRF に表示されるエンドポイント、VRFから消えるエンドポイント、ファブリック内で移動するエンドポイント、ルートリフレクタ接続の喪失、ルートリフレクタ接続の復元などの問題に対して発生します。問題に応じて、アラームポリシーの重大度レベルはCRITICAL またはMINOR になります。

アラームは、次のイベントに対して発生し、CRITICAL に分類されます。

- ルートリフレクタの切断
- 重複する IP アドレスの検出
- 重複する MAC アドレスの検出

次のイベントの場合、アラームが発生し、MINOR として分類されます。

- エンドポイントの移動
- ファブリック内の新しい VRF の表示
- ファブリック内のエンドポイントの数が 0 になる
- VRF のエンドポイントの数が 0 になる
- スイッチからのすべてのエンドポイントの消失
- ルートリフレクタ（RR）の接続

状態が修正されると、CRITICALアラームは自動的にクリアされます。たとえば、NDFC と RR 間の接続が失われると、CRITICAL アラームが生成されます。このアラームは、NDFC と RR 間の接続が回復すると自動的にクリアされます。その他の MINOR アラームは、アラームが生成されてから 30 分が経過すると自動的にクリアされます。

Note 状態が解決されたら、重複する MAC および重複する IP アラームをクリアする必要があります。

[イベント分析（Event Analytics）] > [アラーム（Alarm）] > [アラームポリシー（Alarm Policies）] を選択して、EPL アラームポリシーを表示します。これらのアラームポリシーは、Web UI では編集できません。**[アクション（Actions）] > [アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** を選択して、選択したポリシーをアクティブ化または非アクティブ化します。

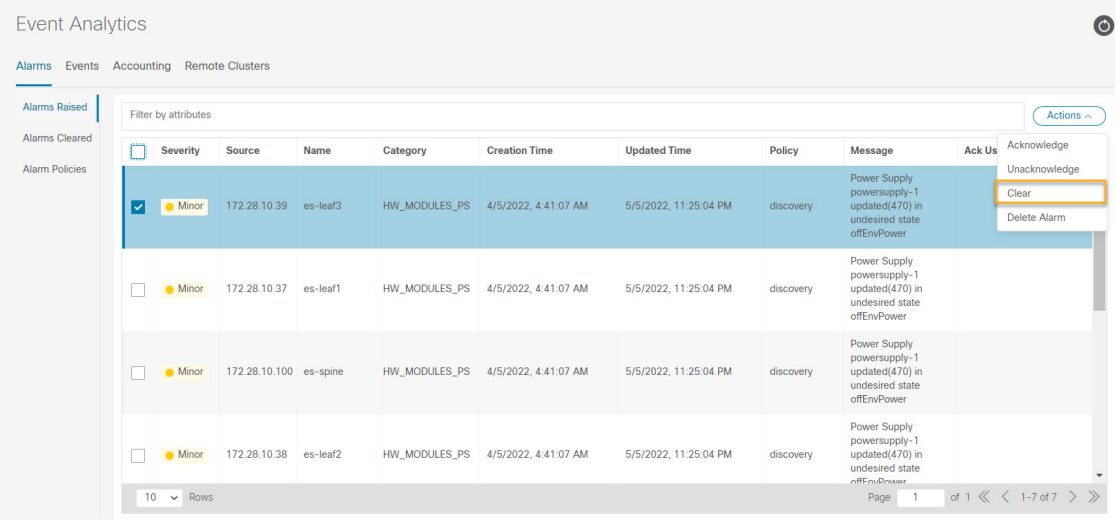
NDFC Web UI を使用してアラームポリシーが削除された場合、そのポリシーに対して作成またはクリアされたアラームは、**[イベント分析（Event Analytics）]>[アラーム（Alarm）]>[アラームポリシー（Alarm Policy）]** タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。ただし、NDFC Web UI からはポリシーを削除しないことをお勧めします。ファブリックが削除される

と、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

エンドポイントロケータ：アクティブアラーム

[イベント分析（Event Analytics）] > [アラーム（Alarm）] > [発生したアラーム（Alarms Raised）] を選択して、アクティブなアラームを表示します。

アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）] > [クリア（Clear）]** をクリックします。

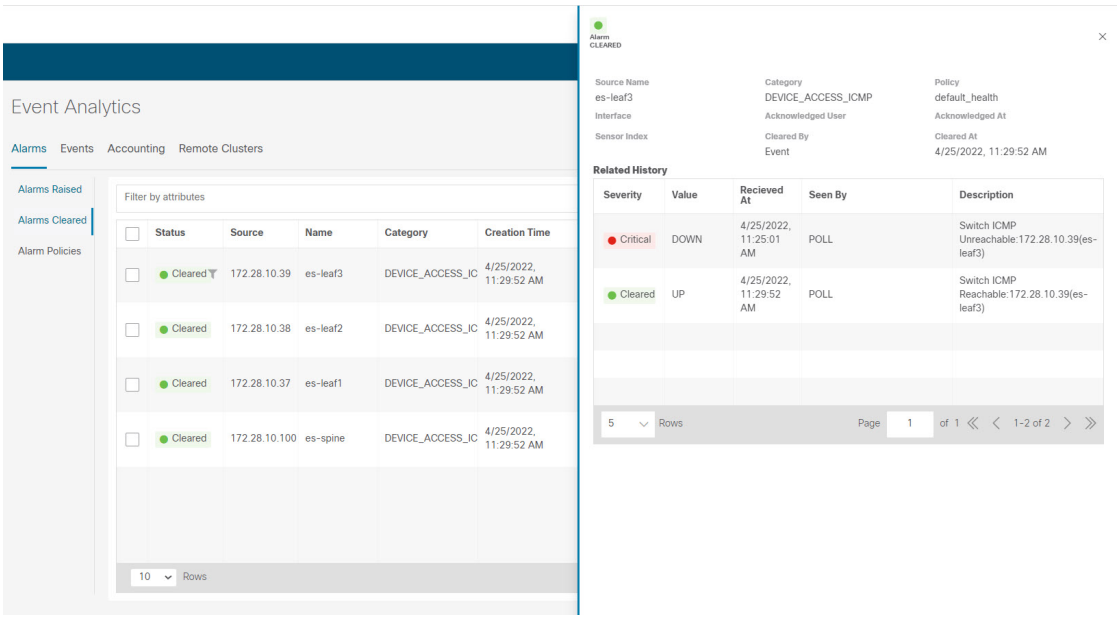


アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）] > [削除（Delete）]** をクリックします。

エンドポイントロケータ：クリアされたアラーム

クリアされたアラームを表示するには、**[イベント分析（Event Analytics）] > [アラーム（Alarms）] > [クリアされたアラーム（Alarms Cleared）]** に移動します。

必要な **[クリア済み（Cleared）]** ステータス列をクリックして、必要なアラームに関する詳細情報を表示します。



クリアされたアラームのリストからクリアされたアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[アクション（Actions）]**>**[削除（Delete）]**をクリックします。

アラームとポリシーの詳細については、「アラーム, on page 207」を参照してください。

San Insights Anomaly ポリシー

Cisco Nexus Dashboard SAN コントローラ リリース 12.0(1) から、新しいポリシータイプ saninsights が追加されました。この新しいポリシータイプは、問題を特定するためにカスタマイズできます。分析のために間隔データごとに保持する特定のフローに基づいて、アラームポリシーを作成できます。選択したフローがアラームポリシーと一致する場合は、ポリシーで定義されたパラメータに基づいてフローを維持します。

手順

ステップ 1 **[操作（Operations）]** > **[イベント分析（Event Analytics）]** > **[アラーム（Alarms）]**の順に選択します。

ステップ 2 **[アラーム（Alarms）]** タブで **[アラーム ポリシー]** を選択します。

ステップ 3 **[アクション（Actions）]** > **[新規アラーム ポリシーの作成（Create new alarm policy）]**の順に選択します。

ステップ 4 **[San Insights の異常ポリシー（San Insights Anomaly Policy）]** オプションボタンを使用します。

ステップ 5 次のパラメータの詳細を指定します。

- **[ポリシー名（Policy Name）]**：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- **[説明（Description）]**：ポリシーの簡単な説明。
- **[転送（Forwarding）]**：外部 SNMP リスナーへの転送アラームを有効にします。

- **[電子メール（Email）]**：このポリシーのメール更新をメール ID に送信するには、チェックボックスを選択します。

ステップ 6 ドロップダウン リストから時間を選択して、**キャプチャ時間**と**保持時間**を定義します。

- **[キャプチャ時間（Capture Time）]**：特定のポリシーに一致する各フローの間隔ごとのデータをキャプチャする時間の長さを指定します。
- **[保持時間（Retention Time）]**：（削除する前に）そのデータを保持する時間の長さを指定します。

ステップ 7 ドロップダウン リストから時間または間隔を選択して**分析レベル**を定義し、ドロップダウン リストから**重大度**レベルを選択してこのポリシーの重大度を定義します。

- **[分析レベル（Analysis Level）]**：特定のポリシーでチェックする必要があるフローデータの集約を指定します。中止ポリシーや失敗ポリシーなどの一部のポリシータイプは、即座に発生する場合に照合するロジックです（間隔レベル）。一部のポリシータイプは、しきい値を超えて維持されると異常ポリシーとして表示されます。たとえば、レベルの瞬間的な ECT または DAL のスパイクはアラームではありませんが、同じスパイク レベルが一定期間（5 分または 1 時間）続く場合は、調査する必要があります。
- **[重大度（Severity）]**：このポリシーが原因で発生するアラームに関連付けられる重大度を指定します。

ステップ 8 新しいルールを定義し、**[新規ルールの追加（Add new rule）]** をクリックして必須フィールドを指定し、**[新規ポリシーの作成（Create new policy）]** をクリックします。

（注）
- 1つ以上の新しいルールと一致基準を定義して、フローを識別し、新しいポリシーを作成できます。
- すべてのポリシーは、スイッチからレシーバにストリーミングされる各 ITL/ITN フロー レコードと照合されます。

作成されたアラームは、**[アラーム（Alarms）]** タブで確認できます。

イベント

このタブには、スイッチに対して生成されたイベントが表示されます。このタブには、Ack、確認済みユーザ、グループ、スイッチ、重大度、ファシリティ、タイプ、カウント、最終確認、説明などの情報が表示されます。1つ以上のイベントを選択し、[ステータスの変更（Change Status）] ドロップダウン リストを使用して、そのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。すべてのイベントを削除する場合は、[すべてを削除（Delete All）] ボタンをクリックします。

次の表で、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるフィールドについて説明します。

フィールド	説明
グループ	ファブリックを指定します。
スイッチ	スイッチのホスト名を指定します。
重大度	イベントの重大度を指定します。
施設	イベントを作成するプロセスを指定します。 イベント ファシリティには、NDFC と syslog ファシリティとの 2 つのカテゴリがあります。 Nexusダッシュボードファブリック コントローラ ファシリティは、Nexusダッシュボード ファブリック コントローラ 内部サービスによって生成されたイベントと、スイッチによって生成された SNMP トラップを表します。syslog ファシリティは、syslog メッセージを作成したマシン プロセスを表します。
タイプ	スイッチ/ファブリックの管理方法を指定します。
数	イベントが発生した回数を提供します。
作成時刻	イベントが作成された時刻を指定します。
前回の検出	イベントが最後に実行された時刻を指定します。
説明	イベントに提供される説明を指定します。
Ack	イベントを確認するかどうかを指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストで、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるアクション項目について説明します。

アクション項目	説明
確認応答あり	テーブルから 1 つ以上のイベントを選択し、**[確認（Acknowledge）]**アイコンを選択して、ファブリックのイベント情報を確認します。 ファブリックのイベントを確認すると、確認アイコンが [グループ（Group）] の横の [Ack] 列に表示されます。
未確認	テーブルから 1 つ以上のイベントを選択し、**[確認解除（Unacknowledge）]** アイコンを選択して、ファブリックのイベント情報を確認します。

アクション項目	説明
削除	イベントを選択し、**[削除（Delete）]** をクリックします。
イベントのセットアップ	では新しいイベントを設定できます。詳細については、イベントのセットアップ（221 ページ）を参照してください。

イベントのセットアップ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 **[操作（Operations）] > [イベント分析（Event Analytics）] > [イベントのセットアップ（Event Setup）]** の順に選択します。**[アクション（Actions）]** ドロップダウン メニューから、**[イベントのセットアップ（Event Setup）]** を選択します。

ステップ 2 [レシーバ（Receiver）] タブで、次の手順を実行します。

a) この機能を有効にするには、トグル ボタンを使用します。

b) **[Syslog メッセージを DB にコピー（Copy Syslog Messages to DB）]**を選択し、**[適用（Apply）]** をクリックして syslog メッセージをデータベースにコピーします。このオプションを選択しない場合、イベントは Web クライアントのイベント ページに表示されません。2 番目のテーブルの列には、次の情報が表示されます。

- トラップを送信するスイッチ
- syslog を送信するスイッチ
- syslog アカウンティングを送信するスイッチ
- 遅延トラップを送信するスイッチ

c) [送信元（Sources）] タブのテーブルには、関連付けられているファブリックとスイッチが表示されます。また、トラップと syslog に関する情報も表示されます。

ステップ 3 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からシステムメッセージの通知転送を追加および削除するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI は、電子メールまたは SNMPv1 トラップを介してファブリック イベントを転送します。一部の SMTP サーバでは、Nexusダッシュボード ファブリック コントローラ から SMTP サーバに送信される電子メールに認証パラメータを追加する必要があります。Nexusダッシュボード ファブリック コントローラ により認証を必要とする任意の SMTP サーバに送信される電子メールに認証パラメータを追加できます。この機能は、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** タブで有効にします。

a) **[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。イベント転送を有効にするには、**[イベント転送を有効にする（Enable Event forwarding）]** チェックボックスをオンにします。イベントの転送範囲、レシーバの電子メールアドレス、イベントの重大度、およびイベントのタイプが表示されます。説明の [正規表現（Regex）] フィールドは、転送送信元がイベント フォワーダの追加時に転送元が Syslog として選択されている場合にのみ適用されます。

b) **SMTP サーバ**の詳細と**送信元**電子メールアドレスを指定します。**スヌーズ**および**イベント カウント** フィルタを設定します。

c) **[Save（保存）]** をクリックします。

d) **[操作（Operations）] > [イベント分析（Event Analytics）]** の順に選択します。[操作（Actions）] ドロップダウン リストから **[ルールの追加（Add Tags）]** を選択します。

e) [転送メソッド（Forwarding Method）] で、**[電子メール]** または **[トラップ（Trap）]** を選択します。

[トラップ（Trap）] を選択した場合は、ダイアログボックスに **[アドレス（Address）** と **[ポート（Port）]** フィールドが追加されます。

f) **電子メール**転送メソッドを選択する場合は、[電子メールアドレス（Email Address）]フィールドに IP アドレスを入力します。**トラップ**メソッドを選択する場合は、[アドレス（Address）] フィールドにトラップ レシーバの IP アドレスを入力し、ポート番号を指定します。

[アドレス（Address）] フィールドに IPv4 または IPv6 アドレスまたは DNS サーバ名を入力できます。

g) **[ファブリック（Fabric）]** フィールドで、通知するすべてのグループまたは特定のファブリックを選択します。SAN インストーラの場合は、**[VSAN 範囲（VSAN Scope）]** を選択します。**[すべて（All）]** または **[リスト（List）]** オプションを選択できます。リストを選択した場合は、通知用の VSAN のリストを指定します。

h) [送信元] フィールドで、Nexusダッシュボード ファブリック コントローラ または **[Syslog]** を選択します。

- Nexusダッシュボード ファブリック コントローラ を選択すると、次のようになります。
  1. **[タイプ（Type）]** ドロップダウン リストから、イベント タイプを選択します。
  2. **[ストレージ ポートのみ（Storage Ports Only）]** チェックボックスをオンにして、ストレージ ポートのみを選択します。
  3. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
  4. **[追加（Add）]** をクリックして、通知を追加します。

- [Syslog] を選択した場合：
  1. **[ファシリティ（Facility）]** リストから、syslog のファシリティを選択します。
  2. syslog **タイプ**を指定します。

3. **[説明の正規表現（Description Regex）]** フィールドで、イベントの説明と一致する説明を指定します。
4. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
5. **[追加（Add）]** をクリックして、通知を追加します。

（注） [最低重大度（Minimum Severity）] オプションは、[イベント タイプ（Event Type）] が **[すべて（All）]** に設定されている場合のみ使用できます。

Cisco Nexusダッシュボード ファブリック コントローラが送信するトラップは、重大度タイプに対応しています。重大度タイプとともにテキストによる説明も提供されます。

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

i) [ルールの追加（Add Rule）] をクリックします。

ステップ 4 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイベント抑制にルールを追加するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ では、ユーザ指定のサプレッサ ルールに基づいて、指定されたイベントを抑制することができます。このようなイベントは、Cisco Nexusダッシュボード ファブリック コントローラ Web UIおよび SAN クライアントには表示されません。イベントは Nexusダッシュボード ファブリック コントローラ データベースに保持されず、電子メールまたは SNMP トラップを介して転送されません。

テーブルからサプレッサ ルールを表示、追加、変更、および削除できます。既存のイベント テーブルからサプレッサ ルールを作成できます。テンプレートとして特定のイベントを選択し、ルール ダイアログウィンドウを呼び出します。イベントの詳細は、イベント テーブルで選択したイベントから、ルール作成ダイアログ ウィンドウの入力フィールドに自動的に移植されます。

（注） Cisco Nexusダッシュボード ファブリック コントローラ Web UI から EMC Call Home イベントを抑制することはできません。

a) ルールの**名前**を指定します。
b) イベント送信元に基づくルールに必要な **[範囲（Scope）]** を選択します。

[範囲（Scope）] ドロップダウン リストには、LAN グループとポート グループが個別に表示されます。**[SAN/LAN]**、**[ポート グループ（Port Groups）]**、または **[任意（Any）]** を選択できます。SAN および LAN の場合は、ファブリックまたはグループまたはスイッチ レベルでイベントの範囲を選択します。ポート グループ スコープのグループのみを選択で

きます。範囲として **[任意（Any）]** を選択すると、サプレッサ ルールがグローバルに適用されます。

c) **ファシリティ**名を入力するか、SAN/LAN スイッチ イベント ファシリティ リストから選択します。

ファシリティを指定しない場合は、ワイルドカードが適用されます。

d) ドロップダウン リストから **[イベント タイプ（Event Type）]** を選択します。

イベント タイプを指定しない場合は、ワイルドカードが適用されます。

e) **[説明の照合（Description Matching）]** フィールドで、一致する文字列または正規表現を指定します。

ルール照合エンジンは、Java パターン クラスでサポートされている正規表現を使用して、イベントの説明テキストとの一致を検索します。

f) **[アクティブ範囲（Active Between）]** ボックスをオンにして、イベントが抑制される有効な時間範囲を選択します。

デフォルトでは、時間範囲は有効になっていません。つまり、ルールは常にアクティブです。

（注） 一般に、アカウンティング イベントを抑制しないでください。アカウンティング イベントの抑制ルールは、アカウンティング イベントが Nexusダッシュボード ファブリック コントローラ またはソフトウェアのスイッチのアクションによって生成される特定のまれな状況でのみ作成できます。たとえば、Nexusダッシュボード ファブリック コントローラと管理対象スイッチ間のパスワード同期中に、多数の「sync-snmp-password」AAA syslog イベントが自動的に生成されます。アカウンティング イベントを抑制するには、[サプレッサ（Suppressor）] テーブルに移動し、[イベント サプレッサ ルールの追加（Add Event Suppressor Rule）] ダイアログ ウィンドウを呼び出します。

g) [ルールの追加（Add Rule）] をクリックします。

アカウンティング

Cisco Nexusダッシュボード ファブリック コントローラ Web UI でアカウンティング情報を表示できます。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）] >** に表示されるフィールドについて説明します。

フィールド	説明
ソース（Source）	送信元 SGT を指定します。
User Name	ユーザ名を指定します。

フィールド	説明
時間	イベントが作成された時刻を指定します。
説明	説明を表示します。
グループ	グループの名前を指定します。

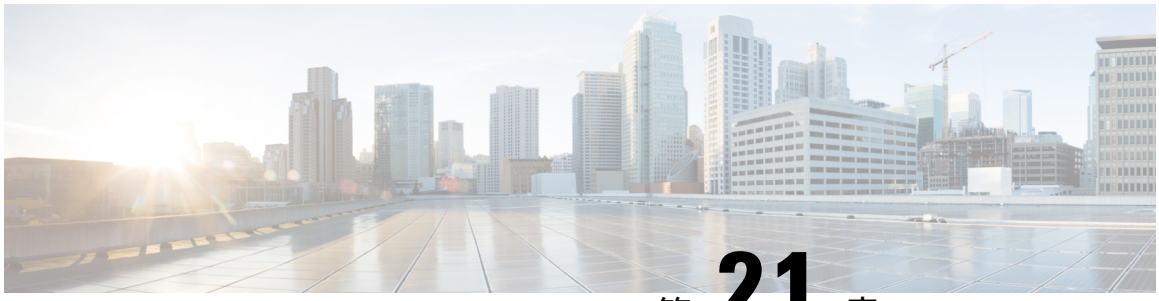
次の表では、**[操作（Actions）]**ドロップダウンリストのアクション項目について説明します。これらの項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）]** に表示されます。

アクション項目	説明
削除	リストからアカウンティング情報を削除するには、行を選択し て**[削除（Delete）]** を選択します。

リモートクラスタ

このタブには、セットアップの各クラスタ内のクラスタとファブリックの数が表示されます。

クラスタ名をクリックして概要情報を表示します。起動アイコンをクリックして、クラスタの詳細な概要を表示できます。



第 21 章

イメージ管理

イメージ管理

デバイスを最新のソフトウェアバージョンに手動でアップグレードすると、時間がかかり、エラーが発生しやすくなります。迅速で信頼性の高いソフトウェアアップグレードを実現するために、イメージ管理はアップグレードの計画、スケジューリング、ダウンロード、およびモニタリングに関連する手順を自動化します。イメージ管理は、Cisco Nexus スイッチでのみサポートされます。

（注） アップグレードする前に、Cisco Nexus 9000 シリーズ スイッチおよび Cisco Nexus 3000 シリーズ スイッチの POAP ブート モードが無効になっていることを確認します。POAP を無効にするには、スイッチ コンソールで [no boot poap enable] コマンドを実行します。ただし、アップグレード後に有効にすることができます。

[イメージ管理（Image Management）] ウィンドウには次のタブがあり、[アクション（Actions）] 列にリストされている操作を実行できます。

タブ	アクション
概要	イメージのステージング イメージの検証 イメージのアップグレード ポリシーの変更 コンプライアンスの再計算
製品イメージ	イメージのアップロード 削除

タブ	アクション
イメージ ポリシー	イメージ ポリシーの作成 削除
履歴	履歴 （239 ページ）

ユーザ ロールが **network-admin** または **device-upg-admin** であり、次の操作を実行するためにNexusダッシュボード ファブリック コントローラをフリーズしていないことを確認します。

- イメージをアップロードまたは削除します。
- イメージのインストール、削除、またはイメージのインストールを終了します。
- パッケージおよびパッチをインストールまたはアンインストールします。
- パッケージおよびパッチをアクティブ化または非アクティブ化します。
- イメージ管理ポリシーを追加または削除します（network-admin ユーザ ロールにのみ適用）。
- 管理ポリシーを表示します。

ユーザ ロールが network-admin、network-stager、network-operator、または device-upg-admin の場合は、任意のイメージインストールまたはデバイスアップグレードタスクを表示できます。Nexusダッシュボード ファブリック コントローラがフリーズ モードの場合は、それらを表示することもできます。

スイッチ イメージをアップグレードするプロセスを次に示します。

1. Nexusダッシュボード ファブリック コントローラへのスイッチを検出します。
2. イメージをアップロードします。
3. イメージ ポリシーを作成します。
4. イメージ ポリシーをスイッチに適用します。
5. スイッチでイメージをステージングします。
6. （任意）スイッチが中断のないアップグレードをサポートしているかどうかを検証します。
7. 適切にスイッチをアップグレードします。

概要

[概要（Overview）] ウィンドウには、シスコ Nexusダッシュボードファブリック コントローラで検出されたすべてのスイッチが表示されます。スイッチの現在のバージョン、スイッチに接続されているポリシー、ステータス、およびその他のイメージ関連情報などの情報を表示できます。エントリをフィルタリングおよびソートできます。

Nexusダッシュボード ファブリック コントローラ UI ナビゲーション

- **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。[アクション（Actions）] をクリックして、さまざまな操作を実行します。

実行するアクションに基づいて、[理由（Reason）] 列の値が更新されます。

[概要（Overview）] ウィンドウで以下のアクションを実行できます。

イメージのステージング

イメージ ポリシーをスイッチに適用した後、イメージをステージングします。イメージをステージングすると、ファイルがブートフラッシュにコピーされます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイメージをステージングするには、次の手順を実行します。

始める前に

- デバイスでイメージをステージングする前に、選択したデバイスにポリシーをアタッチする必要があります。
- SAN コントローラでサポートされる NX-OS イメージの最小バージョンは 6.1(2)I1(1) です。

  上記のバージョンより前の NX-OS バージョンを実行している Nexus 9000 または Nexus 3000 スイッチでイメージをステージングするには、**Use KSTACK to SCP on N9K, N3K** 値を False に設定する必要があります。Web UI で、**[設定（Settings）] > [サーバー設定（Server Settings）] > [SSH]** タブを選択します。**[N9K、N3K で SCP に KSTACK を使用する（Use KSTACK to SCP on N9K, N3K）]** チェック ボックスをオフにします。サポートされているイメージバージョンをステージングする場合は、このチェックボックスをオンにします。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

（注） 複数のスイッチを選択してイメージをステージングできます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[イメージのステージング（Stage Image）]** を選択します。

[インストールするイメージの選択（Select Images to Install）] ウィンドウが表示されます。

このウィンドウでは、スイッチで使用可能な容量と必要な容量を確認できます。

ステップ 4 （任意）[ステージングするファイル（Files For Staging）] 列の下のハイパーリンクをクリックして、ブートフラッシュにコピーされるファイルを表示します。

ステップ 5 **[ステージ（Stage）]** をクリックします。

[イメージ管理（Image Management）] ウィンドウの [概要（Overview）] タブに戻ります。

ステップ 6 （任意）[ステージングするイメージ（Image Staged ）] 列でステータスを確認できます。

ステップ 7 （任意）ログを表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

イメージの検証

スイッチをアップグレードする前に、中断のないアップグレードがサポートされているかどうかを検証できます。Cisco Nexusダッシュボード ファブリック コントローラWeb UI からイメージを検証するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

（注） 複数のスイッチを選択してイメージをステージングできます。

ステップ 3 **[アクション（Actions）]** をクリックして **[検証（Validate）]** を選択します。

[検証（Validate）] ダイアログボックスが表示されます。

ステップ 4 破損のないアップグレード チェックボックスで [確認（Confirm）] にチェックします。

ステップ 5 [**Validate**] をクリックします。

[イメージ管理（Image Management）] ウィンドウの [概要（Overview）] タブに戻ります。

ステップ 6 （任意）[検証済み（Validated）] 列でステータスを確認できます。

ステップ 7 （任意）ログを表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

イメージのアップグレード

スイッチをアップグレードまたはアンインストールできます。アップグレード グループ オプションを使用すると、複数のスイッチでイメージのアップグレードを瞬時にトリガーできます。このオプションは、アップグレード/ダウングレードオプションで選択できます。

（注） 最大 12 個のスイッチを一度にアップグレードすることをお勧めします。12 個を超えるスイッチを選択した場合、アップグレードは順番に実行されます。

NX-OS スイッチのアップグレード オプション

- 中断：中断を伴うアップグレードの場合は、このオプションを選択します。
- [非中断を許可（Allow Non-disruptive）]：中断のないアップグレードを許可する場合に選択します。**[非中断を許可（Allow Non Disruptive）]** オプションを選択し、スイッチが非中断アップグレードをサポートしていない場合、中断アップグレードが実行されます。**[強制中断なし（Force Non Disruptive）]** を選択し、選択したスイッチが中断なしアップグレードをサポートしていない場合、スイッチの選択を確認するよう求める警告メッセージが表示されます。スイッチを選択または削除するには、チェックボックスを使用します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチ イメージをアップグレードするには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション（Actions）]** をクリックし、**[アップグレード（Upgrade）]** を選択します。

[アップグレード/アンインストール（Upgrade / Uninstall）] ウィンドウが表示されます。

ステップ 4 チェックボックスをオンにして、アップグレードのタイプを選択します。

有効なオプションは、NXOS、EPLD、およびパッケージ（RPM / SMU）です。

ステップ 5 NXOS、EPLD、またはパッケージを選択します。

a) アップグレードする方法に基づいて、ドロップダウン リストからアップグレード オプションを選択します。

b) （任意） [BIOS 適用（BIOS Force）] チェックボックスをオンにします。

すべてのデバイスの検証ステータスを表示できます。

c) **[ゴールデン（Golden）]** チェックボックスをオンにして、ゴールデン アップグレードを実行します。

d) **[モジュール番号（Module Number）]** フィールドにモジュール番号を入力します。

このフィールドの下にモジュールのステータスが表示されます。

（注）
- **[パッケージ（Packages）]** を選択すると、パッケージの詳細も表示できます。
- **[アンインストール（Uninstall）]** オプション ボタンを選択して、パッケージをアンインストールできます。

ステップ 6 [アップグレード（Upgrade）] をクリックします。

（注） 複数のスイッチをアップグレードする場合、アップグレード ステータスの更新には 30 ー 40 分かかります。

モードの変更

デバイスのモードを変更できます。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からデバイスのモードを変更するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにして、モードを変更するスイッチを選択します。

（注） 複数のスイッチを選択できます。

ステップ 3 **[アクション（Actions）]** > **[モードの変更（Change Mode）** をクリックします。

[モードの変更（Change Mode）] ダイアログボックスが表示されます。

ステップ 4 ドロップダウン リストからモードを選択します。

有効なオプションは **[標準（Normal）]** と **[メンテナンス（Maintenance）]** です。

ステップ 5 **[保存して続Save and Deploy Now]** または **[Save and Deploy Later]** をクリックします。

[Image Management]ウィンドウの[Overview]タブに戻ります。

ポリシーの変更

スイッチにアタッチしたイメージ ポリシーは更新できます。複数のスイッチのイメージ ポリシーを同時に変更することができます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチにアタッチされたイメージ ポリシーをアタッチまたは変更するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション (Actions)]** をクリックし、**[ポリシーの適用 (Apply Policy)]** を選択します。

ダイアログボックスが表示されます。

ステップ 4 ポリシーをアタッチまたはアタッチ解除するには、必要なチェックボックスを選択します。

ステップ 5 ドロップダウンリストからポリシーを選択します。

ステップ 6 必要に応じて **[アタッチ（Attach）]** または **(アタッチ解除（Detach）]** を選択します。

ステップ 7 （任意）変更を表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

ステップ 8 （任意）[ステータス（Status）] 列の下のハイパーリンクをクリックして、現在のイメージのバージョンと予期されるイメージのバージョンを表示します。

スイッチが **Out-Of-Sync** ステータスの場合は、予期されるイメージのバージョンを表示し、それに応じてスイッチをアップグレードします。

コンプライアンスの再計算

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチの設定コンプライアンスを再計算するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション（Actions）]** をクリックし、**[コンプラアンスの再計算（Recalculate Compliance）]** を選択します。

ステップ 4 変更を表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

レポートの実行

[レポート（Reports）] [レポート定義（Report Definitions）] を選択します。

再度生成する必要があるレポートの横にあるチェックボックスをオンにします。**[アクション（Actions）]** ドロップダウン リストから **[レポートの再実行（Re-run Report）]** を選択して、レポート ジョブを再度実行します。レポート ジョブが再実行されたことを示すポップアップ ウィンドウが表示されます。

[レポートの再実行（Re-run Report）] を使用すれば、スケジュールされた実行時間の前にレポートを生成できます。**オンデマンド ジョブ**の場合は、**[レポートの再実行（Re-run Report）]** をクリックしてレポートを生成します。

製品イメージ

このタブで、イメージとプラットフォームの詳細を表示できます。デバイスにイメージをアップロードまたは削除できます。

次の表で、[操作（Operations）]>[イメージ管理（Image Management）]>[イメージ（Images）]に表示されるフィールドについて説明します。

フィールド	説明
プラットフォーム	プラットフォームの名前を指定します。イメージ、RPM、または SMU は、次のように分類されます。 • N9K/N3k • N6K • N7K • N77K • N5K • その他 • サード パーティ N9K プラットフォームと N3K プラットフォームのイメージは同じです。 アップロードされたイメージが既存のプラットフォームのいずれにもマッピングされていない場合、プラットフォームは [その他（Other）] になります。 プラットフォームは RPM の [サードパーティ（Third Party）] になります。
ビット	イメージのビットを指定します。
イメージ名	アップロードしたイメージ、RPM、または SMU のファイル名を指定します。
イメージのタイプ	イメージ、EPLD、RPM、または SMU のファイルタイプを指定します。
イメージ サブ タイプ	イメージ、EPLD、RPM、または SMU のファイルタイプを指定します。 ファイルタイプ EPLD は [epld] です。イメージのファイル タイプは、[nxos]、[system] または [kickstart] です。RPM のファイルタイプは [feature] で、SMU のファイル タイプは [patch] です。

フィールド	説明
NXOS バージョン	Cisco スイッチのみの NXOS イメージ バージョンを指定します。
イメージ バージョン	Cisco 以外のデバイスを含むすべてのデバイスのイメージ バージョンを指定します。
サイズ（バイト）	イメージ、RPM、または SMU ファイルのサイズをバイト単位で指定します。
Checksum	イメージのチェックサムを指定します。チェックサムは、イメージ、RPM、または SMU のファイルに破損がないかどうかをチェックします。Cisco の Web サイトからダウンロードしたファイルと [イメージのアップロード（Image Upload）] ウィンドウでアップロードしたファイルのチェックサム値が同じかどうかを確認することで、信頼性を検証できます。

次の表に、[アクション（Actions）] メニューのドロップダウンリストで、[操作（Operations）] >[イメージ管理（Image Management）]>[イメージ（Images）]に表示されるアクション項目を示します。

アクション項目	説明
更新	イメージ テーブルを更新します。
アップロード	クリックして新しいイメージをアップロードします。この説明については、イメージのアップロード （235 ページ） を参照してください。
削除	イメージをリポジトリから削除できます。 イメージを選択して、[アクション（Actions）] 、[削除（Delete）] を選択します。確認ウィンドウが表示されます。[はい（Yes）] をクリックして、イメージを削除します。 （注） イメージを削除する前に、イメージにアタッチされているポリシーがどのスイッチにもアタッチされていないことを確認してください。

イメージのアップロード

32 ビットおよび 64 ビットのイメージをアップロードできます。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からサーバにさまざまなタイプのイメージをアップロードするには、次の手順を実行します。

（注） デバイスは、POAP またはイメージのアップグレード中にこれらのイメージを使用します。すべてのイメージ、RPM、および SMU が **[イメージ ポリシー（Image Policies）]** ウィンドウで使用されます。

イメージをアップロードするには、ユーザ ロールが **network-admin** または **device-upg-admin** である必要があります。**network-stager** ユーザ ロールでは、この操作を実行できません。

手順

ステップ 1 **[操作（Operations）]**、**[イメージ管理（Image Management）]**、**[イメージ（Images）]** の順に選択します。

ステップ 2 **[アクション（Actions）]** をクリックし、**[アップロード（Upload）]** を選択します。

[アップロード イメージ（Upload Image）] ダイアログ ボックスが表示されます。

ステップ 3 **[ファイルの選択（Choose file）]** をクリックして、デバイスのローカル リポジトリからファイルを選択します。

ステップ 4 ファイルを選択し、**[OK]** をクリックします。

ZIP または TAR ファイルもアップロードできます。シスコ Nexusダッシュボード ファブリック コントローラ はイメージ ファイルを処理して検証し、それに応じて既存のプラットフォームで分類します。**N9K/N3K**、**N6K**、**N7K**、**N77K**、または **N5K** プラットフォームに該当しない場合、イメージファイルは **サードパーティ** または **その他** のプラットフォームに分類されます。**サードパーティ** プラットフォームは、RPM にのみ適用されます。

ステップ 5 [OK] をクリックします。

EPLD イメージ、RPM、および SMU は、`/var/lib/dcnm/upload/<platform_name>` のリポジトリにアップロードされます。

（注） EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース（Release）] ドロップウンリストが空であるため、ポリシーを作成できません。

すべての NX-OS、キックスタートおよびシステム イメージは、`/var/lib/dcnm/images and/var/lib/dcnm/upload/<platform_name>` のパスのリポジトリにアップロードされます。

ファイル サイズとネットワーク帯域幅によっては、アップロードに時間がかかります。

（注） すべての Cisco Nexus シリーズ スイッチのイメージをアップロードできます。

Cisco Nexus 9000 シリーズ スイッチの EPLD イメージのみをアップロードできます。

ネットワークの速度が遅い場合は、Cisco Nexusダッシュボード ファブリック コントローラ の待機時間を 1 時間に増やして、イメージのアップロードを完了します。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からの待機時間を増やすには、次の手順を実行します。

a) **[設定（Settings）] > [サーバ設定（Server Settings）]** を選択します。
b) **csrf.refresh.time** プロパティを検索し、値を **60** に設定します。

値は分単位です。

c) [Apply Changes] をクリックします。
d) Nexusダッシュボード ファブリック コントローラ サーバを再起動します。

イメージ ポリシー

イメージ管理ポリシーには、RPM または SMU とともに NX-OS イメージの目的の情報が含まれます。ポリシーは特定のプラットフォームに属することができます。スイッチに適用されたポリシーに基づいて、Cisco Nexusダッシュボードファブリック コントローラ では必要な NXOS と RPM または SMU がスイッチに存在するかどうかが確認されます。スイッチ上のポリシーとイメージの間に不一致があると、ファブリック警告が生成されます。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[操作（Operations）] > [イメージ管理（Image Management）] > [イメージポリシー（Images Policies）]** に表示されるアクション項目について説明します。

アクション項目	説明
作成（Create）	イメージに適用できるポリシーを作成できます。イメージ ポリシーの作成 （237 ページ）を参照してください。
Delete	ポリシーを削除できます。 ポリシーを選択して、**[アクション（Actions）]**、**[削除（Delete）]** を選択します。確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックして**ポリシー**を削除します。 （注） デバイスにアタッチされているポリシーを削除しようとすると、エラーメッセージが表示されます。
編集	ポリシーを編集できます。

イメージ ポリシーの作成

Cisco Web UI からイメージ ポリシーを作成するには、次の手順を実行します。 Nexusダッシュボード ファブリック コントローラ

（注） MDS プラットフォームおよび SAN 展開のポリシーを作成する際に、一部のフィールドがグレー表示されます。

始める前に

イメージポリシーを作成する前に、[イメージ（Images）] タブでイメージをアップロードします。イメージのアップロードの詳細については、を参照してください。イメージのアップロード （235 ページ）

手順

ステップ 1 **[操作（Operations）] > [イメージ管理（Image Management）] > [イメージ ポリシー（Image Policies）]** の順に選択します。

ステップ 2 **[アクション（Actions）] > [作成（Create）]** をクリックします。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスが表示されます。

ステップ 3 必要なフィールドに情報を入力します。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名	ポリシー名を入力します。
プラットフォーム	プラットフォーム ドロップダウンリストからプラットフォームを選択します。オプションは、[イメージ（Images）] ウィンドウでアップロードしたイメージに基づいて入力されます。[リリース（Release）] ドロップダウンリストのオプションは、選択したプラットフォームに基づいて自動的に入力されます。
リリース	[リリース（Release）] ドロップダウンリストから NX-OS バージョンを選択します。 64 ビット イメージのリリース バージョンでは、イメージ名に 64 ビットが付加されます。 （注） EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース（Release）] ドロップウンリストが空であるため、ポリシーを作成できません。

フィールド	アクション
パッケージ名	（任意）パッケージを選択します。特定のプラットフォーム（バージョンに依存しない）にアップロードされたすべてのパッケージを表示するには、[パッケージ（Packages）] を選択してから、[すべてのパッケージを表示（View All Packages）] チェックボックスをオンにします。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。
EPLD	（任意）ポリシーが EPLD イメージ用の場合は、[EPLD] チェックボックスをオンにします。
EPLD を選択します	（任意）EPLD イメージを選択します。
RPM の無効化	（任意）パッケージをアンインストールするには、このチェックボックスをオンにします。
アンインストールする RPM	（任意）アンインストールするパッケージをカンマで区切って入力します。[RPM 無効化（RPM Disable）] チェックボックスをオンにした場合にのみ、パッケージ名を入力できます。

ステップ 4 **[Save（保存）]** をクリックします。

次のタスク

デバイスにポリシーをアタッチします。詳細については、ポリシーの変更（232 ページ）セクションを参照してください。

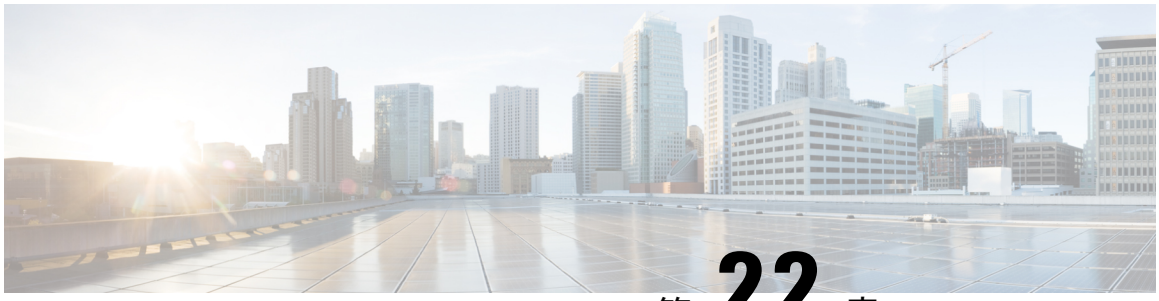
履歴

すべてのイメージ管理操作の履歴は、**[操作（Operations）] [イメージ管理（Image Management）] [履歴（History）]** タブで確認できます。

次の表では、この画面のフィールドについて説明します。

フィールド	説明
ID	ID 番号を指定します。
デバイス名（Device Name）	デバイス名を指定します。
バージョン	デバイスのイメージ バージョンを指定します。
ポリシー名	イメージにアタッチされるポリシー名を指定します。

フィールド	説明
ステータス	操作が成功したか失敗したかを表示します。
理由	操作の失敗の理由を示します。
操作タイプ	実行した操作のタイプを指定します。
Fabric Name（ファブリック名）	ファブリックの名前を指定します。
作成者	操作を実行したユーザー名を指定します。
タイムスタンプ	操作が実行された時刻を指定します。



第 22 章

プログラム可能レポート

[プログラム可能レポート（Programmable Reports）] アプリケーションでは、Python 2.7 スクリプトを使用してレポートを生成できます。レポート ジョブは、レポートを生成するために実行されます。各レポート ジョブは複数のレポートを生成できます。特定のデバイスまたはファブリックに対して実行するレポートをスケジュールできます。これらのレポートは、デバイスに関する詳細情報を取得するために分析されます。

[REPORT] テンプレート タイプは、[プログラム可能レポート（Programmable Reports）] 機能をサポートするために使用されます。このテンプレートには、[UPGRADE] と [GENERIC] の 2 つのテンプレート サブタイプがあります。REPORT テンプレートについて詳細は、レポート テンプレート（299 ページ）を参照してください。レポート生成を簡素化するために Python SDK が提供されています。この SDK はNexusダッシュボード ファブリック コントローラにバンドルされています。

（注） Jython テンプレートは 100k バイトの最大ファイル サイズをサポートします。いずれかのレポート テンプレートがこのサイズを超えると、Jython の実行が失敗する可能性があります。

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

Cisco Nexusダッシュボード ファブリック コントローラ Web UI でプログラム可能なレポートを起動するには、[オペレーション（Operations）] [プログラム可能レポート（Programmable Reports）] を選択します。 >

[レポート（Reports） ウィンドウが表示されます。このウィンドウには、[レポート定義（Report Definitions）] タブと [レポート（Reports）] タブがあります。[レポートの作成（Create Report）] をクリックすると、両方のタブからレポートを作成できます。レポート ジョブの作成については、「レポート ジョブの作成」を参照してください。[更新（Refresh）] アイコンをクリックしてウィンドウを更新します。

（注） Cisco DCNM 11.5 からNexusダッシュボード ファブリック コントローラリリース 12.0.1a にアップグレードした場合、レポート ジョブおよび SAN ユーザ定義レポートは移行されません。手動で再度作成する必要があります。

この章は、次の項で構成されています。

レポートの作成

[操作（Operations）] > **[プログラマブル レポート（Programmable Reports）]**を選択します。[Create Report] をクリックします。**[レポートの作成（Create Report）]** ウィザードが表示されます。

レポート ジョブを作成するには、次の手順を実行します。

手順

ステップ 1 **[レポート名（Report Name）]** フィールドにレポート ジョブの名前を入力します。

ステップ 2 **[Select Template（テンプレートの選択）]** をクリックします。

ステップ 3 ドロップダウン リストからレポート テンプレートを選択し、**[選択（Select）]** をクリックします。

選択したテンプレートに基づいて、画面に表示されるフィールドに必要な値を入力します。

ステップ 4 **[次へ（Next）]** をクリックして、**[ソースと繰り返し（Source & Recurrence）]** のステップに進みます。

ステップ 5 レポート ジョブを実行する頻度を選択します。

次の表に、使用可能なオプションとそれらの説明を示します。

使用可能な方法	説明
現在	レポートは直ちに生成されます
毎日	レポートは、開始日と終了日の間の指定された時刻に毎日生成されます。
毎週	レポートは、開始日と終了日の間に指定された時刻に週に1回生成されます。
毎月	レポートは、開始日と終了日の間に指定された時刻に月に1回生成されます。
Periodic	レポートは、指定された開始日と終了日の間の期間に定期的に生成されます。レポート間の時間間隔は、分単位または時間単位で指定できます。

（注） 定期的な NVE VNI カウンタ レポートを作成する場合は、レポート生成の間隔を 60 分以上に設定する必要があります。間隔が 60 分未満の場合は、エラーメッセージが表示されます。

ステップ 6 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 7 **[デバイスの選択 (Select device(s))]**、**[ファブリックの選択 (Select fabric(s))]**、または **[VSAN の選択 (Select VSAN(s))]** エリアでデバイス、ファブリック、または VSAN を選択します。

（注） 選択したテンプレートに基づいて、デバイス、ファブリック、または VSAN が読み込まれます。

ステップ 8 **[Save（保存）]** をクリックします。

新しいレポートが作成され、**[レポート（Reports）]** タブに表示されます。

レポート テンプレート

各レポート テンプレートには、いくつかのデータが関連付けられています。Nexusダッシュボード ファブリック コントローラ で有効にした機能に応じて、使用可能なレポート テンプレートの一部は次のとおりです。

- Inventory_Report
- Performance_Report
- Switch_Performance_Report
- fabric_cloudsec_oper_status
- fabric_macsec_oper_status
- fabric_nve_vni_counter
- fabric_resources
- sfp_report
- switch_inventory

上記のテンプレートに加えて、作成した他のテンプレートもここに表示されます。デフォルト テンプレートとカスタマイズされたテンプレートの作成の詳細については、「テンプレート ライブラリ」を参照してください。テンプレートは、関連するタグに基づいてリストされます。

Inventory_Report、**Performance_Report**、 **Switch_Performance_Report** は、パフォーマンス管理レポートに使用されます。

レポート定義

[レポート定義（Report Definitions）] タブには、ユーザが作成したレポート ジョブが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル（Title）	レポート ジョブのタイトルを指定します。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	レポートのステータスを指定します。ステータス メッセージは次のとおりです。 • 正常：レポートが正常に生成されました。 • スケジュール済み：レポート生成スケジュールが設定されています。 • 実行中：レポート ジョブが実行中です。 • 失敗：1つ以上の選択されたスイッチ/ファブリックでレポートの実行に失敗したか、レポート ジョブの実行中に問題が発生しました。 • 不明：ジョブの状態を特定できませんでした。
スケジュール	レポートの実行をスケジュールする時刻を指定します。
前回の実行時間（Last Run Time）	レポートが最後に生成された時刻を指定します。
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。

フィールド	説明
内部	レポートがユーザによって生成されるか、ユーザまたは Nexusダッシュボード ファブリック コントローラ によって生成されるかを指定します。レポートがユーザによって生成された場合、値は **false** です。

このタブで次のアクションを実行できます。

（注） 内部レポート定義に対してこれらのアクションを実行することはできません。

アクション	説明
編集	レポートを編集できます。 （注） レポート名とテンプレートは変更できません。
レポートの再実行	レポートを再実行できます。再実行オプションを使用して、スケジュールされた実行時間の前にレポートを生成できます。
履歴	レポート ジョブ履歴を表示できます。 **[ジョブ履歴（Job History）]** ウィンドウが表示されます。レポート ジョブごとに複数のエントリを表示できます。 （注） 表示される定義の数は、**[設定（Settings）] > [サーバ設定（Server Settings）] > [レポート（Reports）]** タブの次の設定によって定義されます。これらの値に基づいて、レポートと履歴が消去されます。 • レポート定義全体の履歴の最大数 • レポート定義あたりの最大レポート数
削除	レポート ジョブを削除できます。

レポート

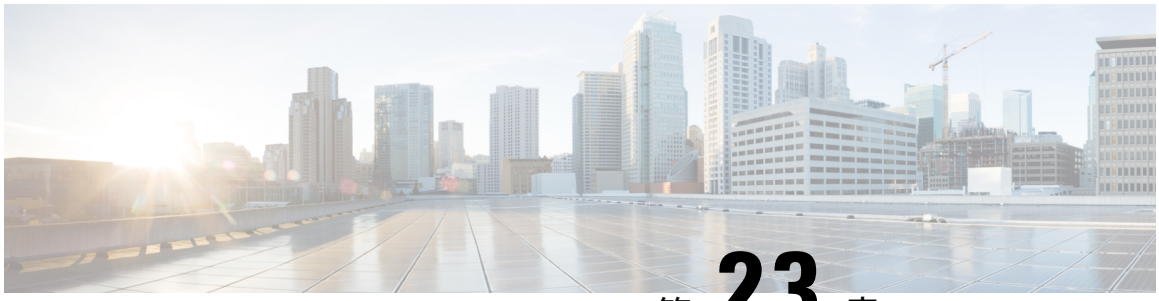
[レポート（Reports）] タブには、ユーザが実行したレポートが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル（Title）	レポートのタイトルを指定します。 • レポートのタイトルを1回クリックすると、サマリー パネルにスライドが表示されます。 • レポートのタイトルをダブルクリックすると、[詳細とコマンド（Details and Commands）] ウィンドウが開きます。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	レポートのステータスを指定します。ステータス メッセージは次のとおりです。 • 完了 • 成功 • 実行中 • FAILED • 警告 • スケジュール済み • 不明ファイル
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。
作成時刻	レポートをいつ作成するかを指定します。
内部	レポートがユーザによって作成されたかどうかを指定します。Nexusダッシュボード ファブリック コントローラレポートがユーザによって作成された場合、値は false です。

このタブで次のアクションを実行できます。

アクション	説明
削除	レポートを削除できます。 （注）　内部レポートは削除できません。
比較（2 レポート）	2つのレポートを並べて比較できます。レポートの詳細は、論理的にセクションにグループ化されます。 コマンドは、デバイスでコマンドを実行するために使用されるテンプレートと API に基づいて表示されます。たとえば、[switch_inventory] テンプレートでは、show version、show inventory、および show license usage コマンドを実行して情報を取得します。コマンドは、show_and_store API を使用してデバイスでコマンドを実行する場合にのみ表示されることに注意してください。
ダウンロード	レポートをダウンロードできます。ダウンロードするレポートを複数選択することはできません。



第 23 章

ライセンス管理

Cisco Nexusダッシュボード ファブリック コントローラ リリース 12.0.1a 以降、次のものからサポートが削除されます。

- 評価ライセンスの状態はサポートされていません。
- サーバ ライセンスファイルはサポートされていません。

  Cisco Smart Software Manager（CSSM）で既存のサーバーライセンスファイルをスマートライセンスに変換する必要があります。詳細については、『Cisco Smart Software Manager』を参照してください。

この章は次のトピックで構成されています。

概要

[操作（Operations）] > **[ライセンス管理（License Management）]** > **[概要（Overview）]**を選択して、既存の Cisco Nexusダッシュボード ファブリック コントローラ のライセンスを表示できます。次のタブでライセンスを表示して割り当てることができます。

- **NDFC**
- **スマート**
- **スイッチ ライセンス ファイル**

（注） デフォルトでは、**[概要（Overview）]** タブが表示されます。

[概要（Overview）] タブには、NDFC、Switch、および Smart の 3 つのカードがあります。これらのカードには、購入するライセンスの総数と期限切れになるライセンスの総数が表示されます。

スマート ライセンシングを有効にするには、**[スマート ライセンシングの設定（Setup Smart Licensing）]** をクリックします。スマート ライセンシングの詳細については、「スマートライセンス」の項を参照してください。

NDFC サーバ ライセンス

NDFC タブでは、各スイッチの NDFC ライセンスのステータスを確認できます。これらのライセンスは、デバイス、スマートライセンス、または名誉ライセンスまたはライセンスのないデバイスでプロビジョニングできます。

1 つまたは複数のスイッチを選択し、**[アクション（Actions）]**、>**[割り当て（Assign）]**または **[すべて割り当て（Assign All）]** をクリックします。

ライセンスをデバイスに割り当てると、NDFC ライセンスサービスは、デバイスの可用性、スマートライセンスのステータス、およびその他の要因に基づいて、使用可能なライセンスを割り当てます。

サーバ ベースのスマート ライセンスは、Cisco MDS スイッチ、Nexus 9000、3000 7000、および 5000 シリーズのスイッチでサポートされます。

ローカル ディレクトリからライセンスを追加するには、次の手順を実行します。

1. [ライセンスの追加（Add license）] をクリックします。

   [ライセンス ファイルの追加（Add License File）] ウィンドウが表示されます。

2. **[ライセンス ファイルの選択（Select License File）]** をクリックし、ローカルディレクトリから適切なファイルを選択します。

3. **[アップロード（Upload）]** をクリックし、**[更新（Refresh）]** アイコンをクリックしてテーブルを更新し、アップロードされたライセンス ファイルを表示します。

   ライセンスファイル名、ライセンスのタイプ、および有効期限の詳細がインポートされたライセンスファイルから抽出され、テーブルに表示されます。

次の表に、**ライセンス管理** > **NDFC** に表示されるフィールドを示します。

フィールド	説明
スイッチ名	スイッチの名前が示されます。

フィールド	説明
License Type	次のいずれかの、スイッチのライセンス ステータスが示されます。 • スイッチ • スマート • スイッチ スマート
ステータス	次のいずれかの、スイッチのライセンス ステータスが示されます。 • 永続 • Unlicensed • スマート • Expired • N/A • 無効
期限日（Expiration Date）	ライセンスの有効期限を指定します。
WWN/シャーシ ID	World Wide Name またはシャーシ ID を表示します。
モデル	デバイスのモデルが示されます。DS-C9124 や N5K-C5020P-BF など。
ファブリック	ファブリックの名前を指定します。

ライセンスを追加するには

次の表では、**[アクション（Actions）]** メニューのドロップダウン リストで、**[ライセンス管理]** > **[NDFC]**に表示されるアクション項目について説明します。

アクション項目	説明
割り当て	スイッチを選択し、**[アクション（Actions）]** ドロップダウンリストから **[割り当て（Assign）]** を選択します。 確認メッセージが表示されます。
割り当て解除	スイッチを選択し、**[アクション（Actions）]** ドロップダウンリストから **[割り当て解除（UnAssign）]** を選択します。 確認メッセージが表示されます。

アクション項目	説明
すべて割り当て	• テーブル内のすべてのスイッチにライセンスを割り当てるには、[Actions]ドロップダウンリストから[Assign All]を選択します。 確認メッセージが表示されます。 • 表を更新するには、**OK** をクリックします。
すべて割り当て解除	• テーブル内のすべてのスイッチにライセンスを割り当て解除するには、**[アクション（Actions）]** ドロップダウンリストから **[すべて割り当て解除（UnAssign All）]** を選択します。 確認メッセージが表示されます。 • 表を更新するには、**OK** をクリックします。

スマートライセンス

Cisco Nexusダッシュボード ファブリック コントローラ では、スマートライセンスを設定することができ、スマートライセンス機能を使用してデバイスレベルでライセンスを管理し、必要に応じてライセンスを更新できます。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（https://software.cisco.com/software/csws/ws/platform/home）。

シスコライセンスの詳細な概要については、https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html を参照してください。

スマートなライセンス管理

Cisco NDFC リリース 12.0.2 から、スマートライセンスポリシーが導入されました。このポリシーはライセンスマイクロサービスで実行され、CSSM を使用して NDFC の高度な機能のライセンスを管理する機能を提供します。このリリースから、スマートライセンスの OnPrem またはオフラインモードを登録できます。

[Smart] ページには、次のカードが表示されます。

- **スマートライセンシングの有効化**

  トグル スイッチを使用して、スマート ライセンシングを有効にします。有効にすると、スマートライセンスは、**信頼の確立**または**オフラインモード**の 2 つの方法で割り当てることができます。

- **信頼ステータス**

  [信頼を確立する（Establish Trust）] をクリックして信頼を確立します。**トランスポートゲートウェイ - CSLU を備えたオンプレミス**を使用し、CSSM を介して Cisco のライセンスサーバーと直接接続するか、**プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ**を経由して接続するかの 2 つのオプションを表示することができます。

  [Smart Licenseの信頼の確立]ウィンドウで、スマートライセンスエージェントとの信頼を確立するときに使用する転送タイプを選択します。

  - シスコ ライセンシング サーバと直接通信するには、**[デフォルト（Default）]**を選択します。
  - **[トランスポートゲートウェイ - CSLU を備えたオンプレミス（Transport Gateway - OnPrem with CSLU）]** を選択し、適切な URL を入力します。

    ライセンスを有効にするために信頼トークンは必要ありません。CSSM とオンプレミス CSLU の間で信頼が確立されます。NDFC およびオンプレミス CSLU から、ローカル接続であることが予想されるため、信頼は一定です。
  - プロキシサーバーを使用して転送するには、**[プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ（Proxy - Proxy via intermediate HTTP or HTTPS proxy）]** を選択します。プロキシ サーバ経由でアクセスするための URL とポートの詳細を入力します。詳細については、CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング （256 ページ）を参照してください。

  デフォルトの転送を使用する場合は、CSSM から取得した登録トークンを入力します。

（注） スマート ライセンシングを登録したら、既存のスイッチにライセンスを手動で割り当てる必要があります。登録後に検出されたすべてのスイッチについて、スマート ライセンシングが自動的にスイッチに割り当てられます。

- **オフライン モード**

オフラインモードでは、NDFCインスタンスとCSSMの間で代替的にデータを共有できます。エアギャップまたは切断された環境で動作している場合、オフラインモードを使用すると、状態をエクスポートしてCSSMにアップロードし、応答をNDFCにインポートして戻すことができます。

ライセンスデータをエクスポートし、CSSMからの応答をインポートするには、以下の手順に従ってください。

1. **[信頼ステータス（Trust Status）]**で**[オフラインモードに切り替える（Switch to Offline mode）]**をクリックして、オフラインモードを有効にします。
2. 1つまたは複数のライセンスが割り当てられているオフラインモードで、**[ライセンスデータのエクスポート（Export License Data）]**をクリックします。
3. https://software.cisco.com/software/csws/ws/platform/home で、スマートライセンスセクションに移動し、**[レポート（Reports）]**タブをクリックして、後続の使用状況データファイルタブを選択します。NDFCからの使用状況レポートをアップロードし、数分後に応答をダウンロードしてNDFCにインポートできます。
4. **[ライセンスデータのインポート（Import License Data）]**をクリックし、CSSM確認応答ファイルをNDFCにアップロードします。

- **ライセンスステータス**

  NDFCのライセンスのステータスを指定します。スマートライセンシングが有効になっていない場合、値は**UNCONFIGURED**です。登録せずにスマートライセンシングを有効にすると、値は**NO LICENSES IN USE**に設定されます。値は、ライセンスを登録して割り当てると、**IN USE**または**NOT IN USE**に設定されます。**[ライセンス認証の詳細（License Authorization Details）]**ポップアップ ウィンドウで、最後のアクション、最後の認証試行、次の認証試行、および認証の有効期限を表示するには、ライセンス ステータスをクリックします。

  ポリシーの詳細をクリックして、スマートライセンスポリシーの詳細を表示します。最初の90日間のデフォルトのスマートライセンスポリシーと、そのレポートから365日以内の現在利用可能なレポートを表示できます。

（注） 最初の登録から30日後にレポートを表示できます。

Resync

NDFCライセンスの総数がCSSMライセンスカウントと同じでない場合は、**[再同期（Resync）]**をクリックしてライセンスカウントを更新します。

再同期により、スイッチインベントリ内のNDFCライセンスのローカル監査が実行され、レポート用にスマートライセンス数が更新されます。

CSSMはスマートライセンスへの従来のライセンスの変換を可能にします。手順については、「https://www.cisco.com/c/dam/en/us/products/se/2020/8/Collateral/brownfield-conversion-qrg.pdf.

ポリシーを使用してスマート ライセンシングからスマート ライセンシングに移行するには、Cisco Nexus Dashboard ファブリック コントローラを起動します。Web UI で、**[オペレーション (Operations)] > [ライセンス管理 (License Management)] > [スマート (Smart)]** タブの順に選択します。SLP を使用して CCSM との信頼を確立します。手順については、「CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング （256 ページ）.

次の表で、「**スイッチ ライセンス**」の項に表示されるフィールドについて説明します。

フィールド	説明
名前	ライセンス名を指定します。
数	使用するライセンスの数を指定します。
ステータス	使用されているライセンスのステータスを指定します。有効な値は、**IN USE** および **NOT IN USE** です。
説明	ライセンスのタイプと詳細を指定します。

ライセンスレポートをアップロードまたはダウンロードするには、https://software.cisco.com/ に移動し、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）] > [Reports（レポート）]** に移動します。**[使用状況データ ファイル（Usage Data Files）]** タブで、**[使用状況データのアップロード（Upload Usage Data）]** をクリックして、NDFC から使用状況レポートをアップロードします。レポートをアップロードしてから数分後、**[確認応答（Acknowledgment）]** 列の **[ダウンロード（Upload Usage Data）]** をクリックして、NDFC に戻されてインポートされた応答をダウンロードします。

スイッチ ライセンス

スイッチがスマートライセンスで事前設定されている場合、Nexusダッシュボードファブリック コントローラ はスイッチのスマート ライセンスを検証して割り当てます。Nexusダッシュボード ファブリック コントローラ Cisco UI を使用してスイッチにライセンスを割り当てるには、**[操作（Operations）] > [ライセンス管理（License Management）] > [スマート（Smart）]** を選択します。スマートライセンスを有効にするには、**[スマートライセンスの有効化（Enable Smart Licensing）]** をクリックします。

スイッチベースのスマートライセンスは、MDSスイッチ、Nexus 9000、および3000 シリーズのスイッチでサポートされます。

（注） 管理対象モードのスイッチの場合は、スイッチのスマートライセンスを Nexusダッシュボード ファブリック コントローラ を介して割り当てる必要があります。

スイッチのスマート ライセンスを有効にするには、Nexusダッシュボード ファブリック コントローラ の手順を実行します。

- 自由形式の CLI 設定を使用して、スイッチでスマート ライセンス機能を有効にします。

- スイッチで feature license smart または license smart enable コマンドを使用して、スマート ライセンシングを構成します。
- license smart register id token コマンドを使用して、デバイスのトークンをスマート アカウントにプッシュします。トークンをプッシュするには、Nexusダッシュボード ファブリック コントローラ で **EXEC** オプションを使用します。

表を更新するには、**更新** アイコンをクリックします。

次の表に、**ライセンス管理** > **スイッチ** に表示されるフィールドを示します。

フィールド	説明
スイッチ	スイッチの名前が示されます。
機能	スイッチの機能を表示します。
ステータス	スイッチが使用中かどうかのステータスを表示します。 • 未使用 • 使用中 • 非準拠
タイプ	次のいずれかの、スイッチのライセンス ステータスが示されます。 • 一時的 • 永続 • スマート • カウンター 永続 • Unlicensed • カウント
Warnings	有効期限など、ライセンスに関する警告を指定します。
グループ	ファブリック名または LAN 名を指定します。

CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング

Cisco Nexus Dashboard ファブリック コントローラのポリシーを使用してスマートライセンシングを使用して CSSM との信頼を確立するには、次の手順を実行します。

始める前に

- Cisco Nexus Dashboard と CSSM の間にネットワーク到達可能性があることを確認します。ネットワーク到達可能性を設定するには、**Cisco Nexus Dashboard Web UI** を起動します。**[管理コンソール（Admin Console）]** で、**[インフラストラクチャ（Infrastructure）] > [クラスタ構成（Cluster Configuration）] > [全般（General）]** タブの順に選択します。**[ルート（Routes）]** 領域で、編集アイコンをクリックし、データ ネットワーク ルートの IP アドレスを追加します。**[保存（Save）]** をクリックして確認します。
- CSSM からトークンを取得していることを確認します。

手順

ステップ 1 **[操作（Operations）] > [ライセンス管理（License Management）] > [Smart]** タブの順に選択します。

ステップ 2 スマート ライセンシングを有効にするには、**[スマート ライセンシングの有効化（Enable Smart Licensing）]** をクリックします。

ステップ 3 **[信頼ステータス（Trust Status）]** カードで、**[信頼の確立（Establish Trust）]** をクリックします。

[スマート ライセンスの信頼の確立（Stablish Trust for Smart License）] ウィンドウが表示されます。

ステップ 4 スマート ライセンス エージェントを登録するには、**[トランスポート（Transport）]** オプションを選択します。

次のオプションがあります。

- **デフォルト：NDFC はシスコのライセンシング サーバーと直接通信します**

  このオプションは、次の URL を使用します。https://smartreceiver.cisco.com/licservice/license

- **トランスポートゲートウェイ：CSLU オプションを備えたオンプレミス**

  CSLU トランスポート URL を入力します。

  （注） CSLU トランスポート URL を使用するには、製品にライセンススマート URL を設定する必要があります。

- **プロキシ：中間 HTTP または HTTPS プロキシ経由のプロキシ**

  このオプションを選択する場合は、URL とポートを入力します。

ステップ 5 **[トークン（Token）]** フィールドに、CSSM から取得したトークンを貼り付けて、スマート ライセンスの信頼を確立します。

ステップ 6 **[信頼の確立（Establish Trust）]** をクリックします。

確認メッセージが表示されます。

ステータスが UNTRUSTED から TRUSTED に変わります。スイッチ ライセンスの名前、数、およびステータスが表示されます。

[TRUSTED] をクリックして詳細を表示します。スイッチの詳細は、[ライセンス割り当て（License Assignments）] タブの [スイッチ/VDC（Switches/VDCs）] セクションで更新されます。スマート ライセンス オプションを使用してライセンスが付与されたスイッチのライセンス タイプとライセンス状態は Smart です。

ステップ 7 **[NDFC]** タブをクリックします。

ステップ 8 [アクション（Actions）] ドロップダウン リストから、**[すべての割り当て（Assign All）]** を選択します。

サーバー ライセンスの **[ステータス (Status)]** に **[コンプライアンス内 (InCompliance)]** が表示されます。

ステータスが **[コンプライアンス外 (OutofComplaince)]** になっている場合は、CSSM ポータルにアクセスして必要なライセンスを取得します。

これ以外のすべてのステータスについては、シスコテクニカルアシスタンスセンター（TAC）にお問い合わせください。

スイッチ ライセンス ファイル

Cisco Nexusダッシュボード ファブリック コントローラ では、1 つのインスタンスで複数のライセンスをアップロードできます。Nexusダッシュボード ファブリック コントローラ はライセンスファイルを解析し、スイッチのシリアル番号を抽出します。検出されたファブリックにライセンスファイルのシリアル番号をマッピングして、各スイッチにライセンスをインストールします。ライセンス ファイルがブート フラッシュに移動され、インストールされます。

次の表では、このタブのフィールドについて説明します。

フィールド	説明
スイッチ	スイッチ名を指定します。
IPのスイッチ	スイッチの IP アドレスを指定します。
ライセンスファイル	ライセンス ファイルのタイプを指定します。
ステータス	ライセンスのステータスを指定します。
Result Message	ライセンスの詳細を指定します。
最終アップロード時刻	サーバにアップロードされた日時を指定します。
機能	ライセンス機能を指定します。

スイッチ ライセンス ファイルの追加

Cisco Nexusダッシュボード ファブリック コントローラ Web Client UI でスイッチにライセンスを一括インストールするには、次の手順を実行します。

手順

ステップ 1 **[操作（Operations）]** > **[ライセンス管理（License Management）]** > **[スイッチ ライセンス ファイル（Switch License Files）]** を選択します。

[スイッチ ライセンス ファイル（Switch License File）] ウィンドウが表示されます。

ステップ 2 [スイッチ ライセンス ファイル（Switch License File）] タブで、**[ライセンスの追加（Add License）]** をクリックして適切なライセンス ファイルをアップロードします。

[ライセンス ファイルの追加（Add License File）] ウィンドウが表示されます。

ステップ 3 [ライセンスファイルの追加]で、[ライセンスファイルの選択]をクリックします。

ローカル ディレクトリにある適切なライセンス ファイルに移動して選択します。

ステップ 4 [アップロード（Upload）] をクリックします。

ライセンス ファイルが Nexusダッシュボード ファブリック コントローラ にアップロードされています。次の情報がライセンス ファイルから抽出されます。

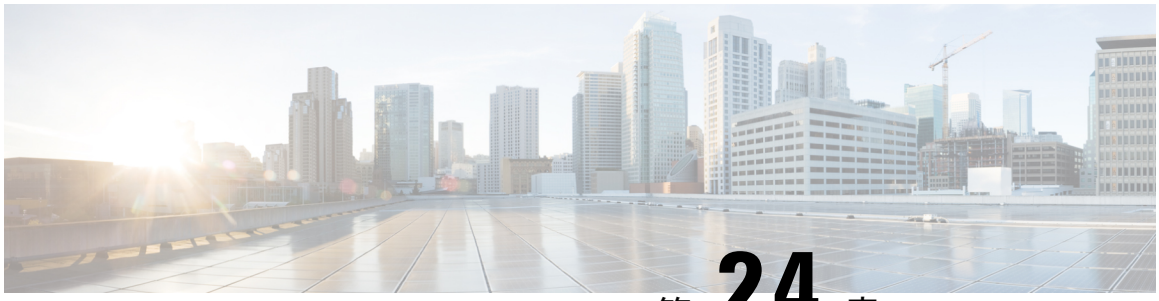
- スイッチ IP：このライセンスが割り当てられているスイッチの IP アドレス。
- ライセンス ファイル：ライセンス ファイルのファイル名
- 機能リスト：ライセンス ファイルでサポートされている機能のリスト

ステップ 5 アップロードし、それぞれのスイッチにインストールするライセンスのセットを選択します。ライセンス ファイルは、単一の特定のスイッチに適用されます。

ステップ 6 **[アクション（Actions）]** > **[インストール（Install）]** をクリックして、ライセンスをインストールします。

選択したライセンスがアップロードされ、それぞれのスイッチにインストールされます。問題やエラーを含むステータスメッセージは、ファイルが完了するたびに更新されます。

ステップ 7 ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ステータス（Status）]** 列にステータスが表示されます。



第 24 章

テンプレート

テンプレート （Templates）

UI ナビゲーション

- **[オペレーション（Operations）] > [テンプレート（Templates）]** を選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントを使用して、異なる Cisco Nexus、IOS-XE、IOS-XR、および Cisco MDS プラットフォームで設定されているテンプレートを追加、編集、または削除できます。Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントで設定されているテンプレートごとに、次のパラメータが表示されます。テンプレートは JavaScript をサポートします。テンプレートの JavaScript 関数を使用して、テンプレートの構文で算術演算と文字列操作を実行できます。

Table 21: テンプレート テーブルのフィールドと説明

フィールド	説明
名前	テンプレート名を指定します。
サポートされるプラットフォーム	テンプレートがサポートするプラットフォームを指定します。
タイプ	テンプレート タイプを指定します。
サブタイプ	テンプレート サブ タイプを指定します。
変更日	テンプレート変更の日時を指定します。
タグ（Tags）	テンプレートがファブリックまたはデバイスにタグ付けされているかどうかを指定します。
説明	テンプレートの説明を指定します。
参照カウント	テンプレートが使用される回数を指定します。

テーブルヘッダーをクリックすると、そのパラメータのアルファベット順にエントリがソートされます。

Note エラーのあるテンプレートは、[テンプレート（Templates）] ウィンドウに表示されません。エラーがあるテンプレートはインポートできません。このようなテンプレートをインポートするには、エラーを修正してインポートします。

次の表では、**[テンプレート（Templates）]** ウィンドウに表示される **[アクション（Actions）]** ドロップダウン リストのアクション項目について説明します。

Table 22: テンプレートのアクションと説明

Actions	説明
新しいテンプレートの作成	新しいテンプレートを作成できるようにします。詳細については、新規テンプレートの作成, on page 264を参照してください。
テンプレートのプロパティの編集	テンプレートのプロパティを編集できるようにします。一度に編集できるテンプレートは1つだけです。詳細については、テンプレートの編集 , on page 266を参照してください。
テンプレートの内容の編集	テンプレートの内容を編集できるようにします。一度に編集できるテンプレートは 1 つだけです。詳細については、テンプレートの編集 , on page 266を参照してください。
テンプレートの複数	選択したテンプレートを別の名前で複製できるようにします。必要に応じて、テンプレートを編集できます。一度に複製できるテンプレートは 1 つだけです。 テンプレートを複製するには、複製するテンプレートの横にあるチェックボックスをオンにし、**[テンプレートの複製（Duplicate template）]** を選択します。**[テンプレートの複製（Duplicate template）]** ウィンドウが表示されます。複製されるテンプレートの名前を指定します。複製されたテンプレートの詳細については、テンプレートの編集 , on page 266を参照してください。

Actions	説明
テンプレートの削除	テンプレートを削除できるようにします。1つのインスタンスで複数のテンプレートを削除できます。 ユーザ定義テンプレートを削除できます。ただし、事前定義されたテンプレートは削除できません。 テンプレートを削除するには、削除するテンプレートの横にあるチェックボックスをオンにし、**[テンプレートの削除（Delete template）]** を選択します。警告メッセージが表示されます。テンプレートを削除する場合は、**[確認（Confirm）]** をクリックします。削除しない場合は、**[キャンセル（Cancel）]** をクリックします。テンプレートが使用中であるか、出荷テンプレートである場合は、削除できず、エラー メッセージが表示されます。 **Note** 複数のテンプレートを選択して、同じインスタンスで削除します。 テンプレートを完全に削除するには、ローカル ディレクトリ `Cisco Systems\dcn\ndfc\data\templates\` にあるテンプレートを削除します。
インポート	ローカル ディレクトリからテンプレートを 1 つずつインポートできます。詳細については、テンプレートのインポート, on page 267を参照してください。

Actions	説明
Zip としてインポート	.zip形式でバンドルされた複数のテンプレートを含む .zip ファイルをインポートできます ZIP ファイル内のすべてのテンプレートが抽出され、個々のテンプレートとしてテーブルにリストされます。 詳細については、「テンプレートのインポート, on page 267」を参照してください。 **Note** Nexusダッシュボード ファブリック コントローラ 仮想アプライアンス（OVAまたはISO）のPOAPテンプレートをインストールするには、POAP テンプレートのインストール, on page 268 を参照してください。 。
エクスポート	ローカル ディレクトリの場所にテンプレート設定をエクスポートできます。一度にエクスポートできるテンプレートは 1 つだけです。 テンプレートをエクスポートするには、テンプレートの横にあるチェックボックスを使用して選択し、**[エクスポート（Export）]** を選択します。テンプレート ファイルを保存するローカル システム ディレクトリの場所を選択します。**[Save（保存）]** をクリックします。テンプレート ファイルがローカル ディレクトリにエクスポートされます。

network-operator ロールを持つテンプレートのみを表示できます。このロールでテンプレートを作成、編集、または保存することはできません。ただし、**network-stager** ロールを使用してテンプレートを作成または編集できます。

この項の内容は、次のとおりです。

新規テンプレートの作成

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からユーザ定義のテンプレートを作成し、ジョブをスケジュールするには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、**[アクション（Actions）]**ドロップダウン リストから **[新規テンプレートの作成（Create new template）]** を選択します。

[テンプレートの作成（Create Template）] ウィンドウが表示されます。

ステップ 2 ウィンドウの **[テンプレート プロパティ（Template Properties）]** ページで、テンプレート名、説明、タグを指定し、新しいテンプレートのサポート対象プラットフォームを選択します。次に、ドロップダウンリストからテンプレートタイプとサブテンプレートタイプを選択します。ドロップダウン リストからテンプレートのコンテンツ タイプを選択します。

Note 基本テンプレートは CLI テンプレートです。

ステップ 3 **[次へ（Next）]** をクリックしてテンプレートの編集を続行するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。

編集したテンプレートのプロパティは、**[テンプレートの編集（Edit Template）]** ウィンドウの **[テンプレート コンテンツ（Template Content）]** ページに表示されます。構成テンプレートの構造については、「テンプレートの構造」の項を参照してください。

ステップ 4 **[検証（Validate）]** をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 5 **[ヘルプ（Help）]** をクリックして、右側の **[エディタ（Help）]** ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。**[エディタのヘルプ（Editor Help）]** ペインを閉じます。

ステップ 6 リンクが表示されたら、**エラー**および**警告**をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に**[エラーおよび警告（Errors & Warnings）]**ペインが表示され、エラーと警告が表示されます。**[エラーおよび警告（Errors & Warnings）]** ペインを閉じます。

ステップ 7 テンプレート コンテンツを作成するには、必要なテーマ、キー バインディング、およびフォント サイズをドロップダウン リストから選択します。

ステップ 8 **[完了（Finish）]** をクリックしてテンプレートの編集を完了し、**[キャンセル（Cancel）]** をクリックして変更を破棄し、**[前へ（Previous）]** をクリックして **[テンプレート プロパティ（Template Properties）]** ページに移動します。

テンプレートが作成されたことを示すメッセージのページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。**[別のテンプレートの作成（Create another template）]** をクリックしてもう 1 つのテンプレートを作成す

るか、**[Edit <template name> template]** をクリックして編集したばかりのテンプレートを編集します。

ステップ 9 **[テンプレートの編集（Edit Template）]** ウィンドウを閉じるか、**[テンプレート ライブラリに戻る（Back to template library）]** をクリックして**[テンプレート（Templates）]** ウィンドウに戻ります。

テンプレートの編集

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

ユーザ定義のテンプレートを編集できます。ただし、定義済みのテンプレートおよびすでに公開されているテンプレートは編集できません。

[テンプレートの編集（Edit Template）] ウィンドウを使用して、最初にテンプレートのプロパティを編集し、次にテンプレートの内容を編集します。さらに、**[テンプレート プロパティの編集（Edit Template Properties）]** アクションを使用してテンプレート プロパティのみを編集するか、**[テンプレート コンテンツの編集（Edit template content）]** アクションを使用してテンプレート コンテンツのみを編集できます。つまり、あるインスタンスでテンプレートのプロパティを編集してから、別のインスタンスでテンプレートの内容を編集できます。このウィンドウを使用して、テンプレートのプロパティとコンテンツを表示することもできます。

テンプレートのプロパティを編集し、テンプレートの内容を編集するには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、テンプレートを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[テンプレート プロパティの編集（Edit Template Properties）]** を選択します。

[テンプレートの編集（Edit Template）] ウィンドウが表示されます。

ステップ 2 ウィンドウの **[テンプレート プロパティ（Template Properties）]** ページに、テンプレートの名前、その説明、サポートされるプラットフォーム、タグ、およびコンテンツ タイプが表示されます。テンプレートの説明とタグを編集できます。サポートされているプラットフォームを編集するには、選択したチェックボックスをオフにして他のスイッチを選択します。次に、ドロップダウン リストからテンプレート タイプとサブテンプレート タイプを選択します。

ステップ 3 **[次へ（Next）]** をクリックしてテンプレートの編集を続行するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。

編集したテンプレートのプロパティは、**[テンプレートの編集（Edit Template）]** ウィンドウの **[テンプレート コンテンツ（Template Content）]** ページに表示されます。

ステップ 4 **[検証（Validate）]** をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 5 **[ヘルプ（Help）]** をクリックして、右側の **[エディタ（Help）]** ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。**[エディタのヘルプ（Editor Help）]** ペインを閉じます。

ステップ 6 リンクが表示されたら、**エラー**および**警告**をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に**[エラーおよび警告（Errors & Warnings）]**ペインが表示され、エラーと警告が表示されます。**[エラーおよび警告（Errors & Warnings）]** ペインを閉じます。

ステップ 7 テンプレート コンテンツを作成するには、必要なテーマ、キー バインディング、およびフォント サイズをドロップダウン リストから選択します。

ステップ 8 **[完了（Finish）]** をクリックしてテンプレートの編集を完了し、**[キャンセル（Cancel）]** をクリックして変更を破棄し、**[前へ（Previous）]** をクリックして **[テンプレート プロパティ（Template Properties）]** ページに移動します。

テンプレートが保存されたことを示すメッセージが表示されたページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。**[別のテンプレートの作成（Create another template）]** をクリックしてもう 1 つのテンプレートを作成するか、**[Edit <template name> template]** をクリックして編集したばかりのテンプレートを編集します。

ステップ 9 **[テンプレートの編集（Edit Template）]** ウィンドウを閉じるか、**[テンプレート ライブラリに戻る（Back to template library）]** をクリックして**[テンプレート（Templates）]** ウィンドウに戻ります。

テンプレートのインポート

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

zip 形式のテンプレートをインポートする場合も、同じ手順に従います。

Note テンプレート内の「\n」は、インポートおよび編集されると改行文字と見なされますが、ZIP ファイルとしてインポートされると正常に機能します。

Note Nexusダッシュボード ファブリック コントローラ 仮想アプライアンス（OVA または ISO）の POAP テンプレートをインストールできます。詳細については、POAP テンプレートのインストール, on page 268を参照してください。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からテンプレートをインポートするには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、**[アクション（Actions）]** ドロップダウンリストから **[テンプレートのインポート（Import template）]** を選択します。

[テンプレートのインポート（Import Template）] ウィンドウが表示されます。

ステップ 2 コンピュータに保存されているテンプレートを参照して選択します。

ステップ 3 **[OK]** をクリックしてテンプレートをインポートするか、**[キャンセル（Cancel）]** をクリックしてテンプレートを破棄します。

Note 圧縮されたテンプレート ファイルをインポートすると、成功またはエラー メッセージが表示されます。**[OK]** をクリックします。

ステップ 4 必要に応じて、テンプレート パラメータとコンテンツを編集できます。詳細については、テンプレートの編集 , on page 266を参照してください。

Note 圧縮されたテンプレート ファイルをインポートすると、**[テンプレートの編集（Edit Template）]** ウィンドウが表示されないことがあります。ただし、必要に応じて **[テンプレートの編集（Edit Template）]** アクションを使用して、テンプレート パラメータとコンテンツを編集できます。

ステップ 5 テンプレートのプロパティまたはコンテンツを編集しない場合は、**[次へ（Next）]**、**[完了（Finish）]**、**[テンプレート ライブラリに戻る（Back to template library）]**の順にクリックして、**[テンプレート（Templates）]** ウィンドウに戻ります。

POAP テンプレートのインストール

UI ナビゲーション

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

Cisco Nexusダッシュボード ファブリック コントローラ では、異なる Cisco Nexus プラットフォームで設定されているユーザ定義テンプレートを追加、編集、または削除できます。Cisco Nexusダッシュボードファブリック コントローラ Release 10.0(x) 以降、シスコ定義の FabricPath および IP VXLAN Programmable Fabric POAP テンプレートは、シスコの公式 Web サイトから

個別にダウンロードできます。これらのテンプレートは、Nexus 2000、Nexus 5000、Nexus 6000、Nexus 7000、およびNexus 9000 シリーズ スイッチで使用する Nexusダッシュボード ファブリック コントローラ 仮想アプライアンス（OVAまたはISO）で使用できます。

シスコ定義のテンプレートは、https://software.cisco.com/download/release.html からダウンロードできます。

Cisco Nexusダッシュボード ファブリック コントローラ から POAP テンプレートをインストールするには、次のタスクを実行します。

手順

ステップ 1 https://software.cisco.com/download/release.html に移動し、ファイルをダウンロードします。

次のいずれかを選択できます。

- `ndfc_ip_vxlan_fabric_templates.10.0.1a.zip`
- `ndfc_fabricpath_fabric_templates.10.0.1a.zip` ファイル

ステップ 2 ファイルを解凍し、コンピューターのローカル ディレクトリに抽出します。

ステップ 3 **[アクション（Actions）]** ドロップダウン リストから **[テンプレートのインポート（Import Template）]** をクリックします。

ステップ 4 コンピュータに保存されているテンプレートを参照して選択します。必要に応じて、テンプレートパラメータを編集できます。

ステップ 5 これらのテンプレートを POAP テンプレートとして指定するには、[**POAP** and **Publish**]チェックボックスをオンにします。

ステップ 6 **[テンプレート構文の検証]** をクリックして、テンプレートを検証します。

ステップ 7 **[保存（Save）]** をクリックしてテンプレートを保存するか、**[保存して終了（Save and Exit）]** をクリックしてテンプレートを保存して終了します。

テンプレート構造

構成テンプレートの内容は、主に4つの部分で構成されます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** の横にある **[ヘルプ（Help）]** アイコンをクリックします。

この項の内容は、次のとおりです。

テンプレートの形式

ここでは、テンプレートの基本情報について説明します。次の表に、使用可能なフィールドの詳細を示します。

プロパティ名	説明	有効な値	任意かどうか
名前（name）	テンプレートの名前	テキスト	いいえ
説明	テンプレートに関する簡単な説明	テキスト（Text）	はい
userDefined	ユーザがテンプレートを作成したかどうかを示します。ユーザが作成した場合、値は「true」です。	「true」または「false」	はい
supportedPlatforms	この設定テンプレートをサポートするデバイスプラットフォームのリスト。すべてのプラットフォームをサポートするには、[All]を指定します。	N1K、N3K、N3500、N4K、N5K、N5500、N5600、N6K、N7K、N9K、MDS、VDC、N9K-9000v、IOS-XE、IOS-XR、その他、すべてのNexusスイッチのリストがカンマで区切られています。	いいえ

プロパティ名	説明	有効な値	任意かどうか
templateType	使用するテンプレートのタイプを指定します。	• CLI • POAP **Note** POAP オプションは、Cisco Nexus ダッシュボードファブリックコントローラ LAN ファブリックの展開には適用されません。 • ポリシー • SHOW • プロファイル • ファブリック • [抽象（ABSTRACT）] • レポート	はい

プロパティ名	説明	有効な値	任意かどうか
templateSubType	テンプレートに関連付けられたサブタイプを指定します。		

プロパティ名	説明	有効な値	任意かどうか
		• CLI • なし • POAP • なし • VXLAN • FABRICPATH • VLAN • PMN **Note** POAP オプションは、Cisco Nexus ダッシュボードファブリックコントローラ LAN ファブリックの展開には適用されません。 • ポリシー • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL	

プロパティ名	説明	有効な値	任意かどうか
		• INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE	

プロパティ名	説明	有効な値	任意かどうか
		• プロファイル • VXLAN • ファブリック • 該当なし • [抽象（ABSTRACT）] • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SUBINTERFACE_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • レポート • アップグレード • GENERIC	

プロパティ名	説明	有効な値	任意かどうか
contentType			はい

プロパティ名	説明	有効な値	任意かどうか
		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI **Note** POAP オプションは、Cisco Nexus ダッシュボードファブリックコントローラ LAN ファブリックの展開には適用されません。 • ポリシー • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • プロファイル • TEMPLATE_CLI • PYTHON • ファブリック • PYTHON	

プロパティ名	説明	有効な値	任意かどうか

		• [抽象（ABSTRACT）]
		  • TEMPLATE_CLI
		  • PYTHON
		• レポート
		  • PYTHON	

実装（Implement）	抽象テンプレートを実装するために使用されます。	テキスト（Text）	はい
依存関係	スイッチの特定の機能を選択するために使用されます。	テキスト（Text）	はい
公開	テンプレートを読み取り専用としてマークし、変更を回避するために使用されます。	「true」または「false」	はい

テンプレート変数

このセクションには、テンプレートに使用されるパラメータの宣言された変数、データ型、デフォルト値、および有効な値の条件が含まれます。これらの宣言された変数は、動的コマンド生成プロセス中にテンプレート コンテンツ セクションの値の置換に使用されます。また、これらの変数は、意思決定およびテンプレート コンテンツ セクションの反復ブロックで使用されます。変数には事前定義されたデータ型があります。変数に関する説明を追加することもできます。次の表に、使用可能なデータ型の構文と使用方法を示します。

変数の型	有効値	反復可能?
boolean	true|false	いいえ
enum	`Example: running-config, startup-config`	いいえ
浮動	浮動小数点形式	いいえ
floatRange	`Example: 10.1,50.01`	はい
整数型（Integer）	任意の数値	いいえ

変数の型	有効値	反復可能?
integerRange	「-」で区切られた連続する番号 「,」で区切られた個別の番号 Example: 1-10,15,18,20	はい
インターフェイス	形式：<if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	いいえ
interfaceRange	Example: eth10/1/20-25, eth11/1-5	はい
IPアドレス	IPv4 または IPv6 アドレス	いいえ
ipAddressList	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	はい
ipAddressWithoutPrefix	Example: 192.168.1.1 または Example: 1:2:3:4:5:6:7:8	いいえ
ipV4Address	IPv4 アドレス	いいえ
ipV4AddressWithSubnet	Example: 192.168.1.1/24	いいえ
ipV6Address	[IPv6アドレス（IPv6 address）]	いいえ

変数の型	有効値	反復可能?
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	いいえ
ipV6AddressWithSubnet	IPv6アドレスとサブネット	いいえ
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	いいえ
long	Example: 100	いいえ
MAC アドレス	14 または 17 文字長の MAC アドレス形式	いいえ

string	変数の説明などに使用される自由テキスト
	
	Example:
	string scheduledTime
	{
	regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;
	}
		いいえ

string[]	Example: {a,b,c,str1,str2}	はい

構造体	単一の変数にバンドルされているパラメータのセット。
	
	struct <structure name declaration > {
	<parameter type> <parameter 1>;
	<parameter type> <parameter 2>;
	…..
	} [<structure_inst1>] [,
	<structure_inst2>] [,
	<structure_array_inst3 []>];
	
	struct interface_detail {
	string inf_name;
	string inf_description;
	ipAddress inf_host;
	enum duplex {
	validValues = auto, full, half;
	};
	}myInterface,
	myInterfaceArray[];
		いいえ
		Note 構造体変数が配列として宣言されている場合、変数は反復型です。

変数の型	有効値	反復可能?
wwn （Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントでのみ使用可能）	Example: 20:01:00:08:02:11:05:03	いいえ

例：テンプレート変数

```
##template variables
integer VSAN_ID;
string SLOT_NUMBER;
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

可変メタ プロパティ

テンプレート変数セクションで定義されている各変数には、一連のメタ プロパティがあります。メタ プロパティは、主に変数に定義されている検証ルールです。

次の表に、使用可能な変数タイプに適用されるさまざまなメタ プロパティを示します。

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
boolean	ブール値。 Example: true	はい											
enum			はい										
浮動	符号付き実数。 Example: 75.56, -8.5	はい	はい	はい	はい	はい							

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
floatRange	符号付き実数の範囲 Example: 50.5 - 54.75	はい	はい	はい	はい	はい							
integer	符号付き実数 Example: 50, -75	はい	はい		はい	はい							
integerRange	符号付き実数の範囲 Example: 50-65	はい	はい		はい	はい							
インターフェイス	インターフェイス/ポートを指定します Example: Ethernet 5/10	はい	はい				はい	はい	はい	はい			
interfaceRange		はい	はい				はい	はい	はい	はい			

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
IPアドレス	IPv4 または IPv6 形式の IP アドレス	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
pAdtsLi		はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: [redacted], [redacted], [redacted] Example 3: 172.22.31.97, 172.22.31.99, [redacted], 172.22.31.254 **Note** リス												

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
		ト内のアドレスは、ハイフンではなくカンマで区切ります。											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	IPv4 または IPv6 アドレス（プレフィックス/サブネットは不要）。												
[illegible]	IPv4 アドレス	はい											
[illegible]	IPv4 アドレスとサブネット	はい											
[illegible]	[IPv6 アドレス（IPv6 addrs）]	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	プレフィックス付き IPv6 アドレス	はい											
[illegible]	IPv6 アドレスとサブネット	はい											
[illegible]	Example: [illegible]												
long	Example: 100	はい			はい	はい							
MAC アドレス	MAC アドレス												
string	リテラル文字列 Example for string Regular expression: string shell line { [illegible] }	はい									はい	はい	はい

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
string[]	カンマ（,）で区切られた文字列リテラル Example: {string1, string2}	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
構造体	単一の変数にバンドルされているパラメータのセット。 struct <structure name> declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [structvar1] [, <structvar2> [, <structvar3> []>];												
wwn	WWN アドレス												

例：メタ プロパティの使用

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

可変注釈

注釈を使用して変数をマーキングする変数プロパティを設定できます。

Note 可変注釈は、POAP でのみ使用できます。ただし、注釈はテンプレートタイプ「CLI」には影響しません。

テンプレート変数セクションでは、次の注釈を使用できます。

注釈キー	有効な値	説明
AutoPopulate	テキスト（Text）	あるフィールドから別のフィールドに値をコピーします。
DataDepend	テキスト	
説明	[テキスト（Text）]	ウィンドウに表示されるフィールドの説明
DisplayName	テキスト（Text） **Note** スペースがある場合は、テキストを引用符で囲みます。	ウィンドウに表示されるフィールドの表示名

注釈キー	有効な値	説明
列挙体	Text1、Text2、Text3 など	選択するテキストまたは数値をリストします
IsAlphaNumeric	「true」または「false」	文字列には、英数字を使用します。
IsAsn	「true」または「false」	
IsDestinationDevice	「true」または「false」	
IsDestinationFabric	「true」または「false」	
IsDestinationInterface	「true」または「false」	
IsDestinationSwitchName	「true」または「false」	
IsDeviceID	「true」または「false」	
IsDot1qId	「true」または「false」	
IsFEXID	「true」または「false」	
IsGateway	「true」または「false」	IPアドレスがゲートウェイかどうかを検証します。
IsInternal	「true」または「false」	フィールドを内部にし、ウィンドウに表示しません。 **Note** この注釈は、ipAddress変数にのみ使用します。
IsManagementIP	「true」または「false」 **Note** この注釈は、変数「ipAddress」に対してのみマークする必要があります。	

注釈キー	有効な値	説明
is_mandatory	「true」または「false」	値をフィールドに強制的に渡す必要があるかどうかを検証します
IsMTU	「true」または「false」	
IsMultiCastGroupAddress	「true」または「false」	
IsMultiLineString	「true」または「false」	文字列フィールドを複数行の文字列テキスト領域に変換します
IsMultiplicity	「true」または「false」	
IsPassword	「true」または「false」	
IsPositive	「true」または「false」	値が正であるかどうかを確認します。
IsReplicationMode	「true」または「false」	
IsShow	「true」または「false」	ウィンドウのフィールドを表示または非表示にします
IsSiteId	「true」または「false」	
IsSourceDevice	「true」または「false」	
IsSourceFabric	「true」または「false」	
IsSourceInterface	「true」または「false」	
IsSourceSwitchName	「true」または「false」	
IsSwitchName	「true」または「false」	
IsRMID	「true」または「false」	
IsVPCDomainID	「true」または「false」	
IsVPCID	「true」または「false」	
IsVPCPeerLinkPort	「true」または「false」	
IsVPCPeerLinkPortChannel	「true」または「false」	

注釈キー	有効な値	説明
IsVPCPortChannel	「true」または「false」	
[パスワード（Password）]	テキスト（Text）	パスワードフィールドを検証します
UsePool	「true」または「false」	
UseDNSReverseLookup		
ユーザ名	テキスト（Text）	ウィンドウにユーザ名フィールドを表示します。
警告	テキスト（Text）	Description 注釈をオーバーライドするテキストを提供します。

例：AutoPopulate 注釈

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

例：DisplayName注釈

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
ipAddress hostAddress;
##
```

例：IsMandatory注釈

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

例：IsMultiLineString注釈

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow注釈

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to
true or false
```

例：警告の注釈

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

テンプレートの内容

この項には、テンプレートで使用する構成コマンドと、すべてのパラメータが含まれています。これらのコマンドには、テンプレート変数セクションで宣言された変数を含めることができます。コマンド生成プロセス中に、変数の値がテンプレートの内容に適切に置き換えられます。

Note 使用するコマンドは、任意のデバイスのグローバル構成コマンドモードで入力するのと同じように指定する必要があります。コマンドを指定するときは、コマンドモードを考慮する必要があります。

テンプレートの内容は、変数の使用によって決まります。

- スカラ変数：反復に使用できない値の範囲または配列を取得しません（変数タイプテーブルでは、 iterate-ableが「No」としてマークされています）。スカラ変数はテンプレートの内容内で定義する必要があります。

  ```
  Syntax: $$<variable name>$$
  Example: $$USER_NAME$$
  ```

- 反復変数：ブロックの反復に使用されます。これらのループ変数は、次に示すように、繰り返しブロック内でアクセスする必要があります。

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- スカラー構造体変数：構造体メンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- 配列構造変数：構造体のメンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

テンプレート変数に加えて、次のステートメントを使用して、条件付きコマンドと反復コマンドの生成を使用できます。

- if-else if-else ステートメント：その中の変数に割り当てられた値に基づいて、設定コマンドのセットの包含/除外を論理的に決定します。

```
Syntax: if(<operand 1>  <logical operator>  <operand 2>){
command1 ..
command2..
..
}
else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- foreach ステートメント：コマンドのブロックを反復するために使用されます。反復は、割り当てられたループ変数値に基づいて実行されます。

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
```

```
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- オプションパラメータ：デフォルトでは、すべてのパラメータが必須です。パラメータをオプションにするには、パラメータに注釈を付ける必要があります。

変数セクションには、次のコマンドを含めることができます。

- **@(IsMandatory=false)**
- **Integer frequency;**

  テンプレートの内容の項では、「if」条件チェックを使用せずに、パラメータに値を割り当てることで、コマンドを除外または含めることができます。オプションのコマンドは、次のように構成できます。

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

高度な機能

次に、テンプレートの構成に使用できる高度な機能を示します。

- 割り当て操作

  構成テンプレートは、テンプレートコンテンツセクション内の変数値の割り当てをサポートします。変数の宣言されたデータ型の値が検証されます。不一致がある場合、値は割り当てられません。

  割り当て操作は、次のガイドラインに従って使用できます。

  - 左側の演算子は、テンプレートパラメータまたはforループパラメータのいずれかである必要があります。
  - 正しい値の演算子は、テンプレートパラメータ、ループパラメータ、引用符で囲まれたリテラル文字列値、または単純な文字列値のいずれかの値です。

  ステートメントがこれらのガイドラインに従っていない場合、またはこの形式に適合しない場合は、割り当て操作とは見なされません。これは、他の通常の行と同様に、コマンド生成時に置き換えられます。

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
```

```
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate メソッド

  設定テンプレートは、Java ランタイムが提供する Java スクリプト環境を使用して、算術演算（ADD、SUBTRACT など）、文字列操作などを実行します。

  テンプレート リポジトリ パスで JavaScript ファイルを見つけます。このファイルには、算術文字列関数の主要なセットが含まれています。カスタム JavaScript メソッドを追加することもできます。

  これらのメソッドは、次の形式の設定テンプレート コンテンツ セクションから呼び出すことができます。

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

  また、次のようなif条件の内部で *evalscript* を呼び出すことができます。

```
if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
do something...
}
```

  Java スクリプト ファイルのバックエンドにあるメソッドを呼び出すことができます。

- 動的な決定

  構成テンプレートは、特殊な内部変数LAST_CMD_RESPONSEを提供します。この変数には、コマンド実行中のデバイスからの最後のコマンド応答が格納されます。これは、デバイスの状態に基づいてコマンドを提供するための動的な決定を行うために、構成テンプレートのコンテンツで使用できます。

Note if ブロックの後には、空の場合もある新しい行で else ブロックを続ける必要があります。

  VLAN がデバイス上に存在しない場合の VLAN の作成例。

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
##
```

  この特別な暗黙的変数は、「IF」ブロックでのみ使用できます。

- テンプレート参照

すべての変数を定義した基本テンプレートを作成できます。この基本テンプレートは、複数のテンプレートにインポートできます。基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。インポートしたテンプレートパラメータと内容は、拡張テンプレート内でアクセスできます。

```
Example: Template Referencing
Base template:
##template properties
 name =a vlan base;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = ;
##
##template variables
 integer vlan_id;
##
##template content
 vlan $$vlan_id$$
##

Derived Template:
##template properties
 name =a vlan extended;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = a vlan base,template2;
##
##template variables
 interface vlanInterface;
##
##template content
 <substitute a vlan base>
 interface $$vlanInterface$$
 <substitute a vlan base>
##
```

拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

レポート テンプレート

REPORT テンプレートのテンプレート タイプは python で、2 つのサブタイプ（UPGRADE と GENERIC）があります。

アップグレード

UPGRADEテンプレートは、ISSU前後のシナリオに使用されます。これらのテンプレートは、ISSU ウィザードに表示されます。

ISSU 前後の処理の詳細については、Nexusダッシュボード ファブリック コントローラ にパッケージ化されているデフォルトのアップグレードテンプレートを参照してください。デフォルトのアップグレード テンプレートは issu_vpc_check です。

GENERIC

GENERIC テンプレートは、リソース、スイッチ インベントリ、SFP、NVE VNI カウンタに関する情報の収集など、一般的なレポート シナリオに使用されます。このテンプレートを使用して、トラブルシューティング レポートを生成することもできます。

リソース レポート

このレポートには、特定のファブリックのリソース使用状況に関する情報が表示されます。

[サマリ（Summary）]セクションには、すべてのリソース プールと現在の使用率が表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。

POOL NAME：プールの名前を指定します。

POOL RANGE：プールの IP アドレス範囲を指定します。

SUBNET MASK：サブネット マスクを指定します。

MAX ENTRIES：プールから割り当て可能な最大エントリ数を示します。

USAGE INSIDE RANGE：プール範囲内に割り当てられている現在のエントリ数を指定します。

USAGE OUTSIDE RANGE：プール範囲外に設定されている現在のエントリ数を指定します。

USAGE PERCENTAGE：これは、(範囲内での使用数/最大エントリ数) *100 という式を使用して計算されます。

[詳細の表示（View Details）]をクリックして、各リソースプールに割り当てられた、または設定されたリソースのビューを表示します。たとえば、SUBNET の詳細セクションには、サブネット内で割り当てられたリソースに関する情報が含まれます。

スイッチ インベントリ レポート

このレポートは、スイッチ インベントリに関する概要を提供します。

[詳細の表示（View Details）] をクリックして、モジュールとライセンスに関する詳細情報を表示します。

SFPレポート

このレポートは、ファブリックおよびデバイス レベルでの SFP の使用率に関する情報を提供します。

（注） スイッチインベントリおよびSFP レポートは、Cisco Nexusデバイスでのみサポートされます。

トラブルシューティング レポート

これらのレポートは、トラブルシューティングのシナリオに役立つように生成されます。現在、定義済みのトラブルシューティング レポートは **NVE VNI** カウンタ レポートのみです。**NVE VNI カウンタ** レポートの生成では、ネットワーク トラフィックに基づいて上位ヒットの

VNIを特定するための定期的なチェックが実行されます。大規模なセットアップでは、レポートの生成頻度を 60 分以上に制限することをお勧めします。

NVE VNI カウンタ レポート

このレポートは、ファブリック内の各 VNI の **show nve vni counters** コマンド出力を収集します。

最も古いレポートと最新のレポートを比較すると、**[サマリ（Summary）]**セクションには上位 10 件のヒット VNI が表示されます。上位ヒット VNI は、次のカテゴリに表示されます。

- ユニキャスト トラフィック用の L2 または L3 VNI
- マルチキャスト トラフィック用の L2 または L3 VNI
- ユニキャスト トラフィック用の L2 のみの VNI
- マルチキャスト トラフィック用の L2 のみの VNI
- ユニキャスト トラフィック用の L3 のみの VNI
- マルチキャスト トラフィック用の L3 のみの VNI

最も古いレポートは、現在のレポート タスクで保存された最初のレポートを参照します。現在のレポートと比較する必要がある最初のレポートとして特定のレポートを選択する場合は、選択したレポートが最初で最も古いレポートになるように、選択したレポートよりも古いすべてのレポートを削除します。

たとえば、昨日の午前 8 時、午後 4 時、および午後 11 時に 3 つのレポートが実行されたとします。今日のレポートの最初の最も古いレポートとして午後 11 時にレポートを使用する場合は、昨日の午前 8 時と午後 4 時に実行されました。

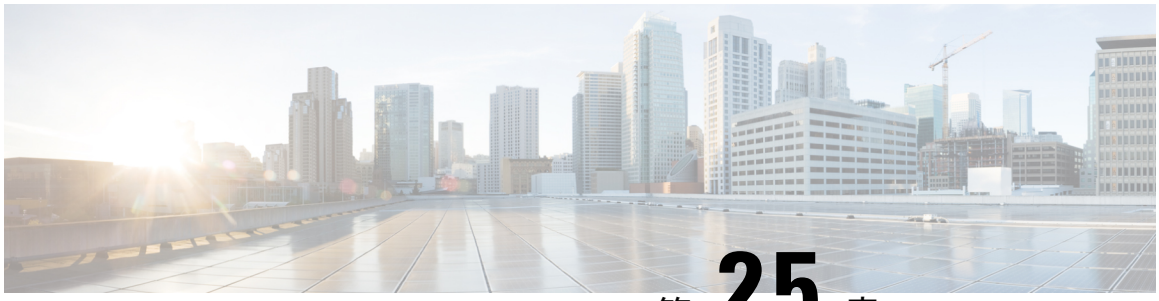
定期レポートの場合、最も古いレポートは、期間の開始時刻に実行される最初のレポートです。日次および週次レポートの場合、現在のレポートが以前に生成されたレポートと比較されます。

[サマリ（Summary）] セクションには、送信された合計バイト数と VNI に関する情報を含むカラムごとのレポートが表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。

（注） NVE VNI カウンタ レポートの **[サマリ（Summary）]** セクションでは、スイッチのリロード後またはスイッチのカウンタのクリア後にレポートが生成された場合、[合計送信バイト数（TOTAL TX BYTES）] 列に負の数が表示されます。番号は、後続のレポートで正しく表示されます。回避策として、スイッチをリロードするか、カウンタをクリアする前に、古いレポートをすべて削除するか、新しいジョブを作成することを推奨します。

詳細については、**[詳細の表示（View Details）]** をクリックしてください。このセクションでは、スイッチごとに NVE VNI とカウンタを示します。

レポートの表示方法の詳細については、「プログラム可能なレポート」の章を参照してください。



第 25 章

テクニカル サポート

テクニカル サポートのログ収集を開始すると、すべてのデータ ストアのクエリが試行されます。システムの現在の状態のスナップショットを作成します。ログの収集が完了すると、通知が表示されます。ログはいつでもダウンロードできます。

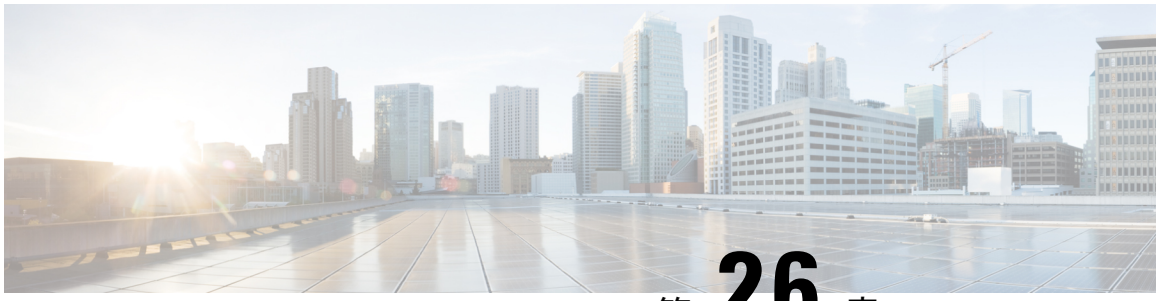
ログ収集

Cisco Nexusダッシュボード ファブリック コントローラ では、トラブルシューティング用のログを収集してダウンロードできます。

[データ収集の開始（Begin data collection）] をクリックして、トラブルシューティングのためにログを収集します。

[ログ収集の再開（Restart log collection）] をクリックして、ログの収集を開始します。この操作により、サーバ上の既存のテクニカル サポート ログが削除されます。収集が完了したら、トラブルシューティングのためにログをダウンロードできます。

[ログのダウンロード（Download log）]をクリックして、ローカル ディレクトリにログをダウンロードします。ログは `.zip` 拡張子でダウンロードされます。



第 26 章

バックアップと復元

いつでも手動でバックアップできます。すべてのファブリック設定とインテントを自動または手動でバックアップするようにスケジューラを設定することもできます。

次のいずれかの形式を使用してバックアップおよび復元できます。

- **設定のみ**：設定のみのバックアップの方が小さくなります。これにはインテント、依存データ、検出情報、ログイン情報、およびポリシーが含まれています。このバックアップからの復元には、機能するファブリック、スイッチの検出、予期される設定、およびその他の設定が含まれています。
- **完全**：フルバックアップは大規模です。これには、現在のデータ、履歴データ、アラーム、ホスト情報、および設定のみのバックアップのすべてが含まれます。このバックアップからの復元には、機能的な履歴レポート、メトリックグラフ、およびすべての基本機能があります。

構成のみのバックアップまたは完全バックアップを復元できます。

バックアップを復元するときは、設定のみの復元または完全な復元を選択できます。設定のみの復元では、設定（インテント、検出情報、ログイン情報、ポリシー）のみが復元され、設定のみのバックアップと完全バックアップの両方を使用して実行できます。完全な復元は、設定と、現在および過去のデータ、チャートなどを復元し、完全バックアップのみを使用して実行できます。

（注） 新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

アップグレード後の機能の互換性

次の表に、NDFC、リリース 12.1.1e へのアップグレード後に DCNM 11.5(x) バックアップから復元される機能に関連する警告を示します。

（注） 11.5(x) には、リリース 11.5(1)、11.5(2)、 のみが含まれます。11.5(4) から 12.1.1e へのアップグレードはサポートされていません。

DCNM 11.5(x) の機能	アップグレードのサポート
vCenter による VMM の可視性	サポート対象
設定されたプレビュー フィーチャー	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
イメージ/イメージ管理データの切り替え	11.5(x) から 12.1.1e に引き継がれない
アラーム ポリシーの設定	11.5(x) から 12.1.1e に引き継がれない
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。

このセクションの内容は次のとおりです。

スケジューラ

スケジューラの目的は、システムを復元する必要がある場合にシステムのバックアップを取ることです。リモートロケーションにバックアップする必要があります。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび設定データのバックアップをスケジュールするには、次の手順を実行します。

始める前に

スケジュールされたバックアップジョブがない場合は、**[スケジュールが設定されていません（No Schedule set）]** が表示されます。

手順

ステップ 1 **[スケジュール設定なし（No Schedule set）]** をクリックします。

[Scheduler（スケジューラ）] ウィンドウが表示されます。

ステップ 2 **[スケジュールされたバックアップの有効化（Enable Scheduled backups）]** チェックボックスをオンにします。

ステップ 3 **[タイプ（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。

ステップ 4 **[ファイル パス（File Path）]** フィールドに、バックアップ ファイルを保存するディレクトリの絶対パスを入力します。

ステップ 5 バックアップディレクトリに**ユーザー名**と**パスワード**を入力します。

ステップ 6 バックアップ ファイルに対する**暗号キー**を入力します。

バックアップから復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

ステップ 7 **[日単位で実行（Run on days）]** フィールドで、チェックボックスをオンにして、1 日以上のバックアップジョブをスケジュールします。

ステップ 8 **[開始時刻（Start at）]** フィールドで、タイムピッカーを使用して特定の時刻にバックアップをスケジュールします。

タイムピッカーは 12 時間制です。

ステップ 9 **[バックアップのスケジュール（Schedule backup）]** をクリックして、スケジュールに従ってバックアップジョブを実行します。

Restore（復元）

（注） 新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

機能が有効になっていない、新しくインストールされた Nexusダッシュボード ファブリック コントローラ でのみ復元を実行できます。

物理的な Nexus Dashboard からバックアップを取得して、仮想 Nexus Dashboard で復元することはできません。

3 ノードクラスタのバックアップを取得して、1 ノードクラスタに復元することはできません。

Cisco Nexusダッシュボード ファブリック コントローラ Web UIからアプリケーションおよび構成データを復元するには、次の手順を実行します。

手順

ステップ 1 [復元（Restore）] をクリックします。

[今すぐ復元（Restore now）] ウィンドウが表示されます。

ステップ 2 **[種類（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。

ステップ 3 （オプション）**[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）]** チェックボックスをオンにします。

[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）] チェック ボックスがオンになっている場合、外部サービスの IP 設定は無視されます。この選択により、システムでバックアップを作成し、それを別の管理サブネットやデータサブネットを持つ別のシステムに復元することができます。

このオプションは、Cisco DCNM 11.5(x) から Cisco NDFC へのアップグレード中には影響しません。

ステップ 4 [復元（Restore）] をクリックします。

バックアップ ファイルが [バックアップと復元（Backup & Restore）] ウィンドウの表に表示されます。復元に必要な時間は、バックアップ ファイルのデータによって異なります。

今すぐバックアップ

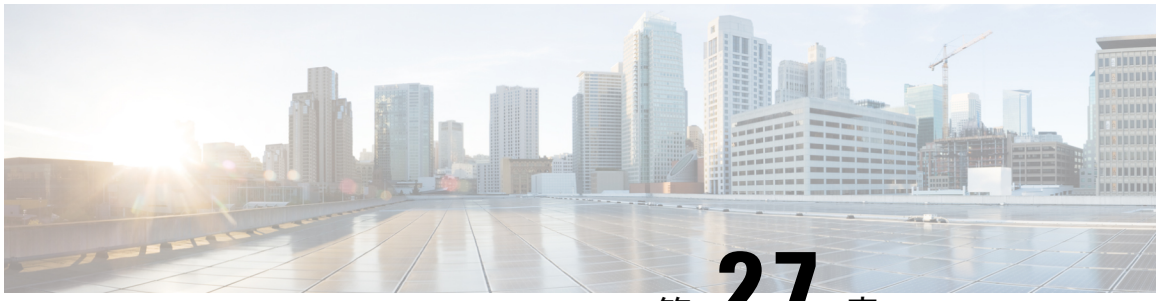
Cisco Nexusダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび設定データのバックアップを取得するには、次の手順を実行します。

手順

ステップ 1 **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 2 **[タイプ（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。



第 27 章

NXAPI 証明書

Cisco NX-OS スイッチを NX-API HTTPS モードで機能させるには、SSL 証明書が必要です。SSL 証明書を生成し、CA によってそれに署名することができます。証明書は、スイッチ コンソールで CLI コマンドを使用して手動でインストールすること、または Cisco Nexusダッシュボード ファブリック コントローラ を使用してスイッチにインストールすることができます。

Cisco Nexusダッシュボード ファブリック コントローラ では、NX-API 証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするための Web UI フレームワークを提供しています。後で、Nexusダッシュボード ファブリック コントローラ によって管理されるスイッチに証明書をインストールできます。

（注） この機能は、Cisco NXOS バージョン 9.2(3) 以降で動作するスイッチでサポートされます。

• 証明書の生成と管理 （309 ページ）

証明書の生成と管理

データセンター管理者は、スイッチごとにASCII（base64）エンコードの証明書を生成します。この証明書は、次の 2 つのファイルで構成されます。

- 秘密キーを含む `.key` ファイル
- 証明書を含む `.crt/.cer/.pem` ファイル

Cisco Nexusダッシュボード ファブリック コントローラ は、組み込みキー ファイル、つまり `.crt/.cer/.pem`ファイルを含む単一の証明書ファイルもサポートします。これには、`.key` ファイルの内容も含めることができます。

Nexusダッシュボード ファブリック コントローラ は、バイナリ エンコードされた証明書はサポートしていません。つまり、`.der` 拡張子の証明書はサポートされません。キー ファイルは、暗号化用のパスワードで保護できます。Cisco Nexusダッシュボード ファブリック コントローラは暗号化を義務付けていません。ただし、これは Nexusダッシュボード ファブリック

コントローラ に保存されるため、キーファイルを暗号化することをお勧めします。Nexusダッシュボード ファブリック コントローラ は AES 暗号化をサポートしています。

CA 署名付き証明書または自己署名証明書のいずれかを選択することができます。Cisco Nexusダッシュボード ファブリック コントローラ は署名を義務付けていません。ただし、セキュリティ ガイドラインでは、CA 署名付き証明書を使用することを推奨しています。

複数のスイッチ用に複数の証明書を生成して、Nexusダッシュボードファブリック コントローラにアップロードすることができます。証明書に適したスイッチを選択できるように、証明書に適切な名前を付けてください。

1 つの証明書と対応するキーファイルをアップロードすることも、複数の証明書とキーファイルを一括アップロードすることもできます。アップロードが完了したら、スイッチにインストールする前に、アップロード リストを確認することができます。組み込みキー ファイルを含む証明書ファイルがアップロードされた場合、Nexusダッシュボード ファブリック コントローラ は自動的にキーを取得します。

証明書とキーファイルは同じファイル名である必要があります。たとえば、証明書ファイル名が `mycert.pem` の場合、キーファイル名は `mycert.key` である必要があります。証明書とキー ペアのファイル名が同じでない場合、Nexusダッシュボード ファブリック コントローラはスイッチに証明書をインストールできません。

Cisco Nexusダッシュボード ファブリック コントローラ では、スイッチに証明書を一括インストールできます。一括インストールでは同じパスワードが使用されるため、すべての暗号化キーは同じパスワードで暗号化する必要があります。キーのパスワードが異なる場合、証明書を一括モードでインストールすることはできません。一括モードインストールでは、暗号化されたキー証明書と暗号化されていないキー証明書を一緒にインストールできますが、すべての暗号化キーは同じパスワードを持つ必要があります。

スイッチに新しい証明書をインストールすると、既存の証明書が新しい証明書に置き換えられます。

同じ証明書を複数のスイッチにインストールすることができます。ただし、一括アップロード機能は使用できません。

（注） Nexusダッシュボード ファブリック コントローラ は、提供される証明書またはオプションが有効であることを要求しません。この規則に従うかどうかは、ユーザーとスイッチの要件次第です。たとえば、スイッチ 1 のための証明書が生成されても、それがスイッチ 2 にインストールされた場合、Nexusダッシュボード ファブリック コントローラ は証明書の適用を強制しません。スイッチは、証明書のパラメータに基づいて証明書を受け入れるか、拒否するかを選択できます。

Cisco Nexusダッシュボード ファブリック コントローラ による NX-API 証明書の検証

リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ はスイッチによって提供される NX-API 証明書を検証する機能をサポートしています。Cisco Nexusダッシュボード ファブリック コントローラ が行う NX-API リクエストには SSL 接続が必要です。ス

イッチはSSLサーバーのように動作し、SSLネゴシエーションの一部としてサーバー証明書を提供します。対応する CA 証明書が提供されている場合、Cisco Nexusダッシュボード ファブリック コントローラ はそれを確認できます。

（注） デフォルトでは、NX-API 証明書の検証は有効にされていません。これは、データセンター内のすべてのスイッチに CA 署名付き証明書がインストールされている必要があり、Cisco Nexusダッシュボード ファブリック コントローラ には対応するすべての CA 証明書が供給されるためです。

Cisco Nexusダッシュボード ファブリック コントローラ の NX-API 証明書管理には、同じ対象を管理するためのスイッチ証明書とCA 証明書という 2 つの機能があります。

スイッチ証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切な証明書ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラにアップロードする必要がある証明書キーペアを選択します。

   拡張子が `.cer/.crt/.pem` および `.key` の証明書を個別に選択できます。

   Cisco Nexusダッシュボード ファブリック コントローラ では、埋め込みキーファイルを含む単一の証明書ファイルをアップロードすることもできます。キーファイルはアップロード後に自動的に取得されます。
3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ にアップロードします。

   ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

   テーブルには、ステータスが UPLOADED と表示されます。証明書がキーファイルなしでアップロードされた場合、ステータスは KEY_MISSING と表示されます。

スイッチの割り当てと証明書のインストール

Cisco Nexusダッシュボード ファブリック コントローラ Web UIを使用してスイッチに証明書をインストールするには、次の手順を実行します。

1. 1 つまたは複数の証明書のチェックボックスをオンにします。

2. **[アクション (Actions)]** ドロップダウンリストから、**[スイッチの割り当てとインストール (Assign Switch & Install)]** を選択します。
3. **[NX API 証明書クレデンシャル (NX API Certificate Credentials)]** フィールドに、証明書の生成時にキーを暗号化するために使用したパスワードを入力します。

   [パスワード (Password)] フィールドは必須ですが、キーがパスワードを使用して暗号化されていない場合は、任意のランダムな文字列を入力できます（たとえばtest、installなど）。暗号化されていないファイルの場合、パスワードは使用されませんが、一括モードであるため、ランダムな文字列を入力する必要があります。

（注） 1 回の一括インストールで、暗号化されていないキーと暗号化されたキーおよび証明書をインストールできます。ただし、暗号化キーに使用するキーパスワードを指定する必要があります。

4. 証明書ごとに、**[割り当て (Assign)]** の矢印をクリックし、証明書に関連付けるスイッチを選択します。
5. **[証明書のインストール (Install Certificates)]** をクリックして、それぞれのスイッチにすべての証明書をインストールします。

証明書のリンク解除と削除

証明書をスイッチにインストールすると、Nexusダッシュボードファブリック コントローラは Nexusダッシュボードファブリック コントローラから証明書をアンインストールできません。ただし、スイッチにはいつでも新しい証明書をインストールできます。スイッチにインストールされていない証明書は削除できます。スイッチにインストールされている証明書を削除するには、スイッチから証明書のリンクを解除してから、Nexusダッシュボードファブリック コントローラから削除する必要があります。

（注） スイッチから証明書のリンクを解除しても、スイッチの証明書は削除されません。証明書はまだスイッチに存在します。Cisco Nexusダッシュボード ファブリック コントローラ はスイッチの証明書を削除できません。

Nexusダッシュボード ファブリック コントローラ リポジトリから証明書を削除するには、次の手順を実行します。

1. 削除する必要がある証明書を選択します。
2. **[アクション (Actions)]** ドロップダウン リストから、**[リンク解除 (Unlink)]** を選択します

   確認メッセージが表示されます。
3. **[OK]** をクリックして、選択した証明書をスイッチからリンク解除します。

ステータス カラムには [UPLOADED] と表示されます。[Switch] カラムには [NOT_INSTALLED] と表示されます。

4. [Switch] から、現在リンク解除されている証明書を選択します。
5. **[アクション (Actions)]** ドロップダウン リストから、**[削除 (Delete)]** を選択します。

   証明書は Nexusダッシュボード ファブリック コントローラ から削除されます。

CA 証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切なライセンス ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラにアップロードする証明書とキーのペアを選択します。

   ファイル拡張子が `.cer/.crt/.pem` ファイル拡張子をもつ証明書を個別に選択できます。

（注） CA 証明書は公開証明書であり、キーは含まれません。また、この操作にはキーは必要ありません。これは、スイッチが提供するNX-API証明書を確認するためにCisco Nexusダッシュボードファブリック コントローラが必要とする証明書です。つまり、CA 証明書はCisco Nexusダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ にアップロードします。

   ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

スイッチの割り当てと証明書のインストール

これらのCA 証明書は Cisco Nexusダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

証明書のリンク解除と削除

CA 証明書はスイッチにインストールされないため、リンク解除する必要はありません。

CA 証明書は、特定の CA に新しい証明書を持ち込む必要があるため、削除できます。

[アクション (Actions)] ドロップダウン リストから、**[削除 (Delete)]** を選択します。証明書はNexusダッシュボード ファブリック コントローラ から削除されます。

NX-API 証明書検証の有効化

NX-API 証明書の検証は、[CA 証明書] ページのトグル ボタンを使用して有効にできます。ただし、これは、Cisco Nexusダッシュボード ファブリック コントローラ が管理するすべてのスイッチに CA 署名付き証明書がインストールされ、対応する CA ルート証明書（1つ以上）がCisco Nexusダッシュボード ファブリック コントローラ にアップロードされた後にのみ行う必要があります。これを有効にすると、Cisco Nexusダッシュボード ファブリック コントローラSSLクライアントはスイッチによって提供される証明書の検証を開始します。検証に失敗すると、NX-API コールも失敗します。

（注）

- NX-API 証明書の検証は、スイッチごとに適用できません。 all または none のいずれかです。したがって、すべてのスイッチに対応する CA 署名付き証明書がインストールされている場合にのみ、検証を有効にすることが重要です。
- また、すべての CA 証明書が Cisco Nexusダッシュボード ファブリック コントローラ にインストールされている必要があります。
- 検証の問題が原因で特定のスイッチでNX-API コールが失敗した場合は、トグル ボタンを使用して適用を無効にできます。すべての結果は、以前の状態に戻ります。
- 上記の点から、メンテナンス期間中に適用を有効にする必要があります。