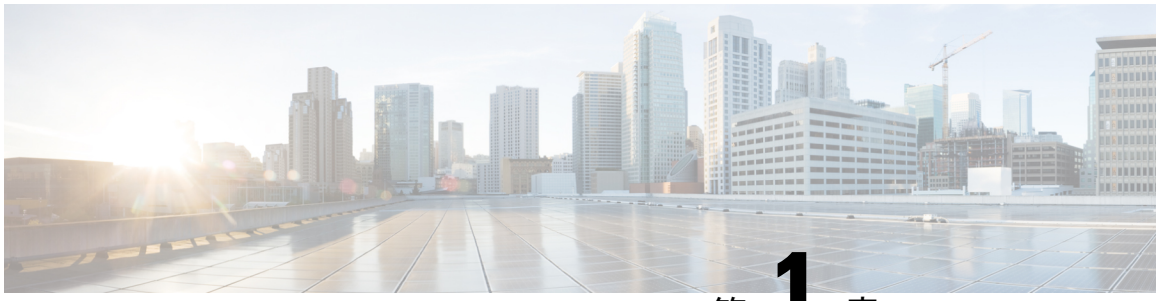
Cisco DCNM SAN 管理 [構成ガイド（Configuration Guide）]、リリース 11.5(x)

初版：2020 年 12 月 23 日

最終更新：2022 年 3 月 4 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/

目 次



第 1 章

[概要（Overview）]

Cisco Data Center Network Manager

Cisco Data Center Network Manager（Cisco DCNM）は、Cisco Nexus 5000、6000、7000、および 9000 シリーズ スイッチと Cisco MDS 9000 シリーズ スイッチのインフラストラクチャを自動化します。Cisco DCNM では、制御、自動化、モニタリング、視覚化、トラブルシューティングなどのすぐに使用できる機能を提供しながら、複数のデバイスを管理できます。

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

Cisco DCNM を LAN ファブリック モードで展開している場合、デバイス コネクタの構成は必須です。インストール時にデバイス コネクタを構成しなかった場合は、ログインするたびにデバイス コネクタを構成するように求めるメッセージが表示されます。**[次回から表示しない（Do not show again）]** にチェックを入れると、メッセージは表示されません。ただし、**[アラーム（Alarms）]** アイコンの下にアラーム通知が追加されます。

Cisco DCNM ホームページの左側にはナビゲーション ペインがあり、中央のペインにはいくつかの Cisco DCNM 機能へのショートカットがあります。

このガイドでは、Cisco DCNM SAN 展開の UI 機能に関する包括的な情報を提供します。

上部ペインには、次の UI 要素が表示されます。

- **[ヘルプ（Help）]**: 文脈依存オンライン ヘルプを起動します。

- **[検索（Search）]**：次の検索条件に従ってレコードを見つけるのに役立ちます。
  - Name
  - IP アドレス
  - WWN
  - Alias
  - MAC アドレス
  - シリアル番号
- [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。
- **[歯車（Gear）]**アイコン: 歯車アイコンをクリックして、次のオプションを含むドロップダウン リストを表示します。
  - **[選択したユーザーとしてログイン（Logged in as）]**：現在ログインしているユーザーのユーザー ロールを表示します。
  - **DCNM SAN & DM**：クリックして、SAN クライアントとデバイス マネージャのセットアップをダウンロードします。管理用にFMクライアントとデバイスマネージャをインストールできます。

    システムのJavaキャッシュは、古いバージョンのDCNMを記憶しています。したがって、DCNM SANおよびDMに最新バージョンをダウンロードするときは、アプリケーションを起動する前に Java キャッシュをクリアしてください。
  - **[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 （network administrator）]ユーザの場合、他のユーザーのパスワードを変更できます。
  - **[詳細（About）]**：バージョン、インストール タイプ、および Web UI が動作してからの時間を表示します。
  - **[REST API ツール（REST API Tool）]**：すべての操作で呼び出された API を調べることができます。API検査についてもっと詳しい情報を得るには*[REST API ツール（REST API Tool）]* セクションを表示します。
  - **[ログアウト（Logout）]**：Web UI を終了し、ログイン画面に戻ります。

Cisco DCNM の詳細については、次を参照してください：

https://www.cisco.com/c/en/us/support/cloud-systems-management/data-center-network-manager-11/model.html.

REST API ツール

Cisco DCNM Web UI で実行される検出、ファブリック管理、モニタリングなどの操作では、アクセスされた情報をフェッチしてコミットするために HTTP 呼び出しを行います。REST API ツールを使用すると、API 呼び出しの構造を表示して API 呼び出しを調べることができます。このツールは、対応する CURL リクエストも提供し、迅速なプロトタイプの作成と API のテストを支援します。

[REST API ツール（REST API Tool）] ダイアログ ボックスには、次のフィールドがあります。

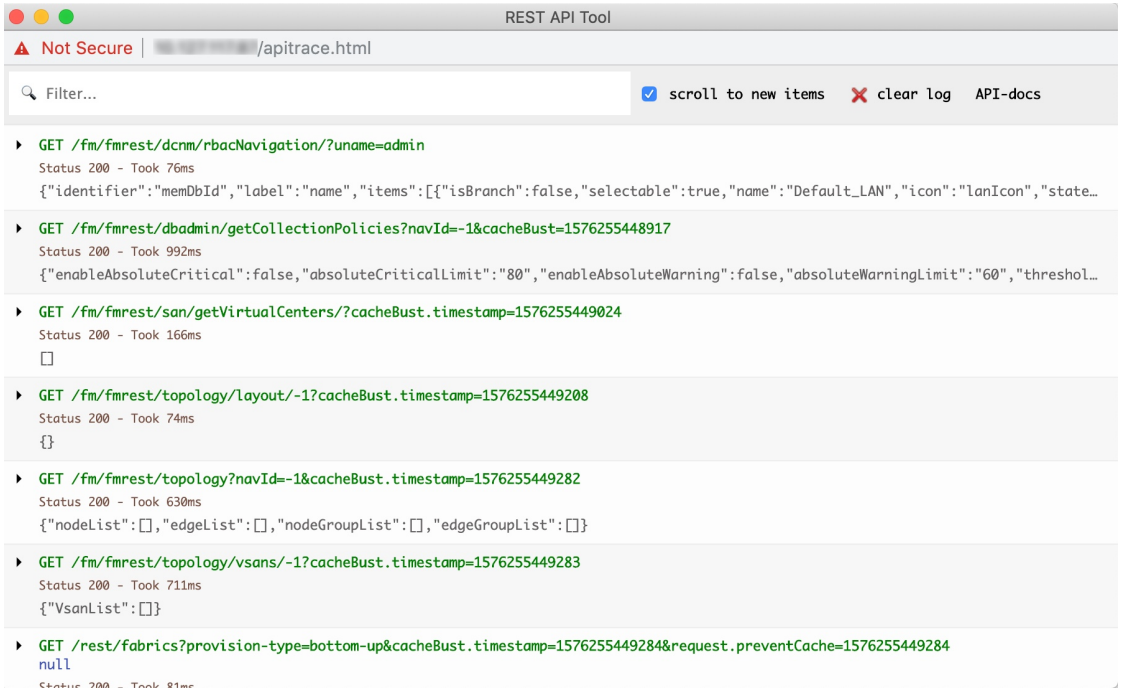
***Table 1: REST API* ツール ダイアログ ボックスのフィールドと説明**

フィールド	説明
フィルタ	任意のキーワードを入力してログを検索します。
新しいアイテムにスクロール	Web UI で操作を実行した後、**[REST API ツール（REST API Tool）]** ダイアログ ボックスに戻ったときに、新しいエントリにスクロールするには、このチェック ボックスをオンにします。 このチェックボックスは、デフォルトでオンになっています。
clear log	**[ログのクリア（clear log）]** をクリックして、ダイアログ ボックスのログをクリアします。
API ドキュメント	API-docs をクリックして、Web UI で Cisco DCNM REST API ドキュメントを表示します。このオプションをクリックすると、次の URL に移動します。https://*DCNM-IP*/api-docs

Cisco DCNM Web UI で実行するすべてのアクションは、API インスペクタ ツールに表示されます。次の情報は、すべての操作で呼び出される API に表示されます。

- HTTPメソッド
- URI
- ペイロード
- HTTP ステータス コード
- 操作にかかる時間

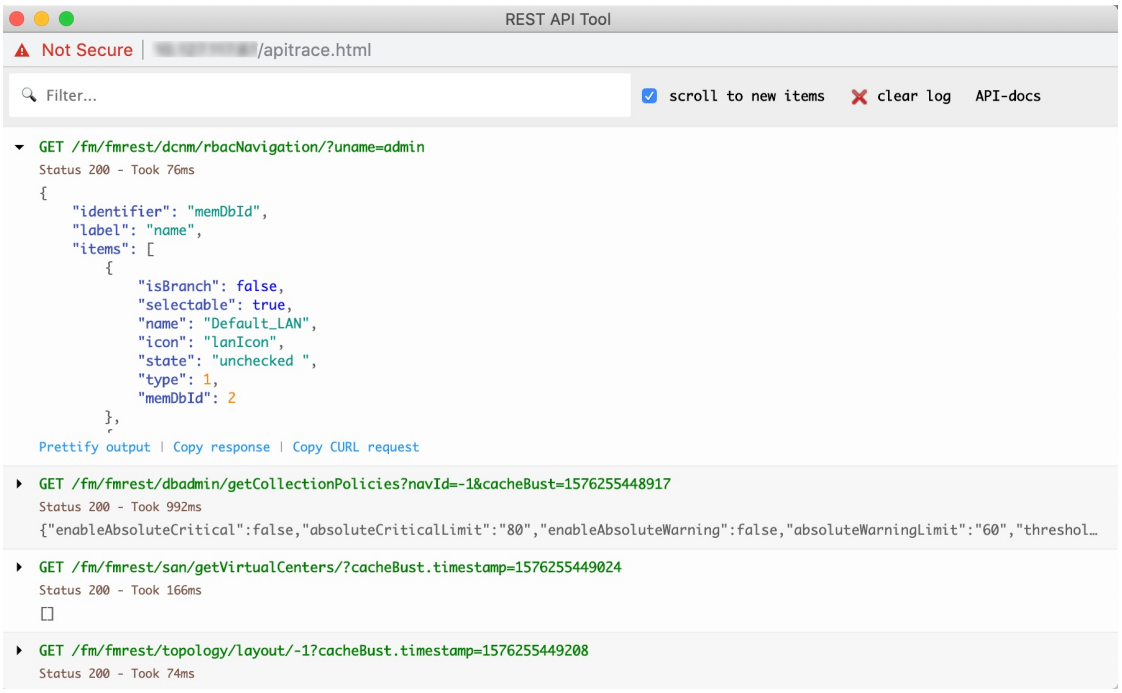
次の画像は、**[REST API ツール（REST API Tool）]** ダイアログ ボックスにログがどのように表示されるかを示しています。



各 REST メソッドを展開または折りたたむには、URI をクリックします。REST メソッドを展開した後、次のアクションを実行できます。

- **出力を整形する**：このオプションをクリックして、応答コードをより見やすいように配置します。そうしないと、1行で表示されます。応答をスクロールして、完全に表示します。
- **応答をコピー**：このオプションをクリックして、応答コードをクリップボードにコピーします。
- **CURL リクエストをコピー**：このオプションをクリックして、CURL リクエストをクリップボードにコピーします。

```
curl -k -XGET --header 'Dcnm-Token: <DCNM_TOKEN>' --header 'Content-Type:
application/x-www-form-urlencoded'
https://<ip-address>/fm/fmrest/dcnm/rbacNavigation/?uname=admin
```



[REST API ツール（REST API Tool）] ダイアログ ボックスは、Cisco DCNM Web UI が更新されるたびに更新されます。

Cisco DCNM Web UI から API インスペクタを使用するには、次の手順を実行します。

Procedure

ステップ 1 上部ペインの**歯車**アイコンをクリックします。

ステップ 2 ドロップダウン リストから **[REST API ツール（REST API Tool）]** を選択します。

Cisco DCNM Web UI で操作を実行する前は、**[REST API ツール（REST API Tool）]** ダイアログ ボックスが表示されており、ログは空です。

ステップ 3 **[REST API ツール（REST API Tool）]** ダイアログ ボックスを最小化します。

Note ダイアログボックスを開いたままにすることもできますが、閉じないようにすることもできます。

ステップ 4 Cisco DCNM Web UI で操作を実行します。

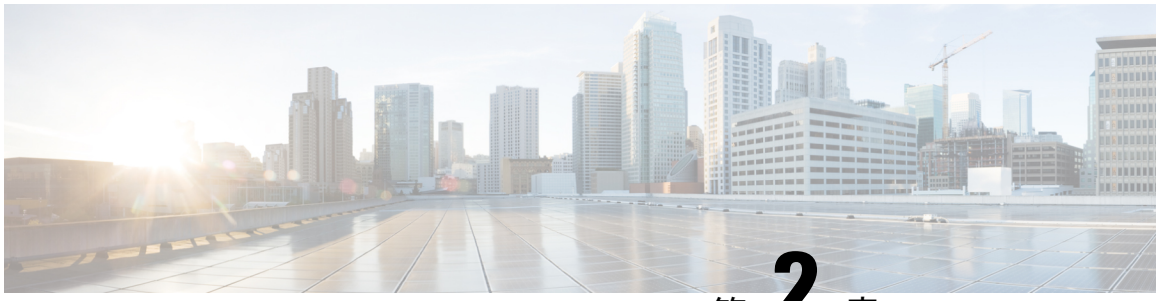
Note オプションの表示、追加、削除など、Cisco DCNM Web UI で任意の操作を実行できます。

ステップ 5 **[REST API ツール（REST API Tool）]** ダイアログ ボックスに戻ります。

ログには、実行した操作に応じてフェッチされた REST API が入力されます。

Note 操作を実行する前に **[REST API ツール（REST API Tool）]** ダイアログ ボックスを最小化するのではなく閉じてしまうと、ログがクリアされます。

REST API ツールを使用して実行できる操作の一部のデモについては、Cisco DCNM ビデオでの REST API ツールの使用を参照してください。



第 2 章

ダッシュボード

この章は次のトピックで構成されています。

[要約（Summary ）]ダッシュボード

[要約（Summary）][ダッシュボード（Dashboard）]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エリア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。ローカル エリア ネットワーク（LAN）[と SAN（and SAN）] スイッチングの機能ビューは、デフォルトで選択された範囲のコンテキストで情報を表示する [9つ（nine）]のダイナミック ダッシュレットで構成されます。ウィンドウの右上隅で範囲を調整して、管理対象ドメインに固有のフォーカスされた情報を表示できます。データ センターの範囲の一部である特定のトポロジまたはトポロジの設定の詳細を提供します。

Cisco Data Center Network Manager (DCNM) Web インターフェイスで使用できるさまざまな範囲は次のとおりです。

- **データセンター**
- **Default_SAN**
- **Default_LAN**
- 各 SAN ファブリック
- 作成するカスタム 範囲

左のメニュー バーから **[ダッシュボード > サマリ（Dashboard > Summary）]** を選択します。**[Summary（サマリ）]** ウィンドウには、次のデフォルト ダッシュレットが表示されます。

[サマリ（Summary）] 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。

- 正常性
- イベント
- アラーム
- 上位の ISL/ポート チャネル
- 上位の SAN エンドポート
- SAN Insights
- エラー
- 破棄
- インベントリ – ポート容量

[ダッシュレット（Dashlets）] ドロップダウン リストから、さらにダッシュレットを選択して、[サマリ（Summary）] ダッシュボードに追加できます。

パネルを追加、削除、ドラッグして並べ替えることができます。

ダッシュレット

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に自動的に表示されます。ダッシュボードに自動的に表示されないダッシュレットを追加するには、Cisco DCNM Web UI から、次の手順を実行します。

Procedure

ステップ 1 **[ダッシュボード（Dashboard）] > [概要（Summary）]** を選択します。

ステップ 2 **[ダッシュレット（Dashlets）]** ドロップダウン リストから、ダッシュボードに追加するダッシュレットを選択します。

[ダッシュレット（Dashlets）] ドロップダウン リストで、選択したダッシュレットの前にアイコンが表示されます。

次の表に、**[概要（Summary）][ダッシュボード（Dashboard）]** ウィンドウに追加できるダッシュレットを示します。

ダッシュレット	説明
Events	重大度が**重大**、**エラー**、および**警告**のイベントを表示します。このダッシュレットで、**[確認済みイベントの表示（Show Acknowledged Events）]** リンクをクリックして、**[モニタ**

ダッシュレット	説明
	（Monitor）] > [スイッチ（Switch）] > [イベント（Events）] に移動します。
アラーム	**重大、メジャー、マイナー**および**警告**の重大度のアラームを表示します。このダッシュレットで、**[確認済みアラームの表示（Show Acknowledged Alarms）]** リンクをクリックして、**[モニタ（Monitor）] > [アラーム（Alarms）] > [表示（View）]** ウィンドウに移動します。特定のアラームの詳細については、青い **[i]** アイコンにマウス カーソルを合わせます。特定のアラームを確認するには、**[ACK]** をクリックします。
リンク トラフィック	データセンターで送受信するための Inter-Switch Link（ISL）およびサチュレーション リンクの図を表示します。
データセンタ	現在の範囲内の各スイッチ グループのアクセス、スパインおよびリーフ デバイスの数、および一般的な正常性スコアを表示します。デバイスは、スイッチ グループ内のタイプ別に集約されます。
監査ログ	Cisco DCNM のアカウンティング ログ テーブルを表示します。
ネットワーク マップ	Role Based Access Control（RBAC）範囲で表示される設定済みのスイッチ グループを世界地図に表示します。範囲セレクタを使用すると、表示されるスイッチ グループのセットが制限されます。[デタッチ（detach）] オプションをクリックすると、マップが新しいタブで開き、構成できます。 • [ネットワーク マップ（network map）] ダイアログ ボックスには、サマリー ダッシュボード ビューとは異なるプロパティがあります。 • ノードをクリックしてドラッグすると、マップ内でノードを移動できます。マップは新しい位置を保存します。 • ノードをダブルクリックすると、特定のスイッチ グループに関するインベントリ

ダッシュレット	説明
	サマリーの情報を含むスライダーをトリガできます。 • 選択した画像をネットワーク マップの背景としてアップロードできます。 **Note** 現在のウィンドウサイズである推奨サイズの画像ファイルをアップロードするように求められます。リセットは、ネットワークマップをデフォルトの状態に戻し、ノードの位置をリセットし、カスタム画像をクリアします。
サーバー ステータス	DCNMおよびフェデレーションサーバーのステータス、およびコンポーネントの正常性チェック ステータスを表示します。 次のサービス、サーバー、およびステータスの詳細が **[DCNM]** タブに表示されます。 • データベース サーバー • 検索インジケータ • パフォーマンスコレクタ • NTPD サーバー • DHCP サーバー • SNMP トラップ • Syslog サーバー **[正常性チェック（Health Check）]** タブには、次のコンポーネントのステータスと詳細が表示されます。 • AMQP サーバー • DHCP サーバー • TFTP サーバー • EPLS • EPLC

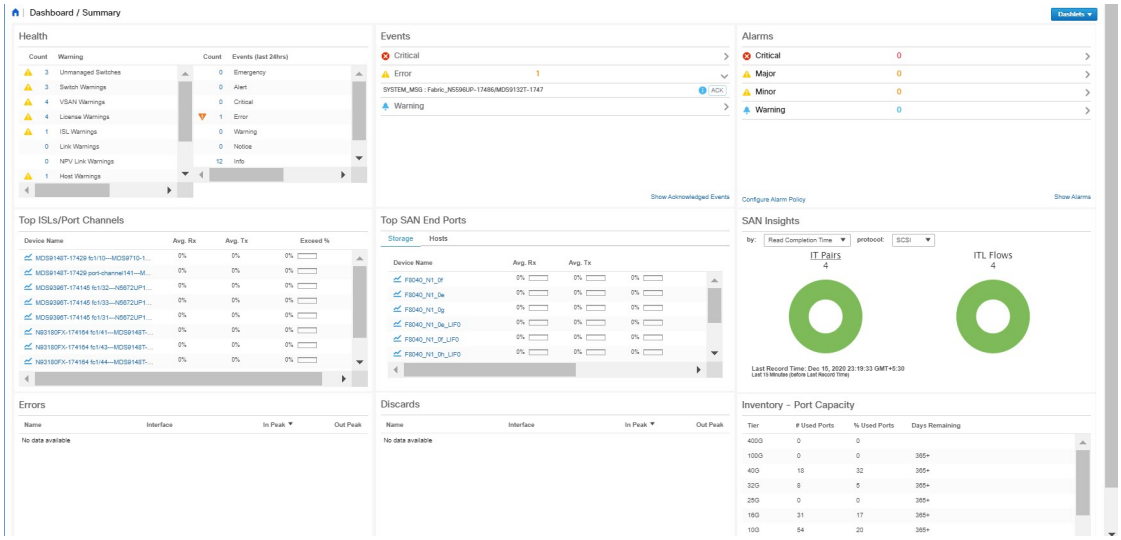
ダッシュレット	説明
上位 ISL/トランク	パフォーマンスの上位 10 個の ISL、トランクポート、またはその両方のパフォーマンスデータを表示します。各エントリには、現在の平均の受信と送信の割合が表示され、各トランクが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。
上位の SAN エンドポート（SAN のみ）	パフォーマンスが高い上位 10 位までの SAN ホストおよびストレージポートのパフォーマンスデータを表示します。各エントリには、現在の受信と送信の割合が表示され、各トランクが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。 **Note** このダッシュレットは SAN 専用です。
上位 CPU	過去 24 時間に検出されたスイッチの CPU 使用率を表示し、赤いバーにその 24 時間の最高水準点を表示します。
上位パラメータ	スイッチのモジュール温度センサの詳細を表示します。 **Note** このダッシュレットは LAN 専用です。
正常性	過去 24 時間の問題のサマリーとイベントの要約を表示する 2 つの列を含む正常性のサマリーを表示します。 スイッチ、ISL、ホスト、またはストレージ（0 以外）に関する警告の横にあるカウントをクリックして、そのファブリックの対応するインベントリを表示します。 イベントの重大度レベル（緊急、アラート、重大、エラー、警告、通知、情報、またはデバッグ）の横にあるカウントをクリックして、対応するイベントのサマリーと説明を表示します。 リリース 11.4(1) 以降、Cisco DCNM を HA モードで展開している場合、正常性ダッシュレッ

ダッシュレット	説明
	トに HA セットアップのステータスが表示されます。HA状態とともに、アクティブ、スタンバイ HA ノード、および VIP の IP アドレスも表示されます。
エラー	選択されたインターフェイスのエラー パケットを表示します。この情報は、**[モニタ（Monitor）] > [LAN/イーサネット（LAN / Ethernet）]** ページの **[エラー（Errors）] > [In-Peak]** および **[エラー（Errors）] > [Out-Peak]** 列から取得されます。
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。 **Note** 破棄ダッシュレットは LAN 専用です。
インベントリ（ポート）	ポートインベントリに関する要約情報を表示します。
インベントリ（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。
インベントリ（ISL）	ISL のカテゴリや数など、ISL インベントリのサマリー情報を表示します。
インベントリ (論理)	論理リンクのカテゴリや数など、論理インベントリのサマリー情報を表示します。
インベントリ（スイッチ）	スイッチ モデルや対応するカウントなど、スイッチのインベントリ サマリー情報を表示します。
インベントリ（ポート容量）	階層、使用可能なポートの数と割合、残りの日数など、ポート容量インベントリ サマリー情報を表示します。
SAN Insights フロー（SAN のみ）	次のようなドーナツを表示します。 • **[プロトコル（protocol）]** ドロップダウンリストから SCSI プロトコルが選択されている場合の **Initiator-Target (IT) Pairs** および **Initiator-Target-LUN(ITL Flows)** のフローのサマリー。

ダッシュレット	説明
	• **[プロトコル（protocol）]** ドロップダウン リストから NVMe プロトコルが選択されている場合の **Initiator-Target (IT) Pairs** および **Initiator-Target-Namespace (ITN Flows)** のフローのサマリー。 ドロップダウン リストから必要なオプションを選択して、読み取り完了時間または書き込み完了時間のデータを表示できます。ドーナツのセクションにカーソルを合わせると、偏差のパーセンテージ値が表示されます。パーセンテージ値は、san.telemetry.deviation.low/med/high、san.telemetry.nvme.deviation.low/med/high、および san.telemetry.default.protocol サーバー プロパティを変更することで、要件に応じて構成できます。 データポイントは、Elasticsearchデータベース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。選択した**範囲**について、elasticsearch のデータが 15 分より古い場合、**[最終記録時間（Last Record Time）]** は赤で表示されます。 SAN Insights の詳細については、「SAN Insights の導入」を参照してください。 **Note** このダッシュレットは SAN 専用です。
上位 FICON ホスト ポート	上位 10 個の FICON チャネル（CH）ポートを実行する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。
上位 FICON 制御ユニット ポート	上位 10 個の FICON 制御ユニット（CH）ポートを実行する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

ダッシュレット	説明
	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。
上位 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。

Note ダッシュボードページでデフォルトのダッシュレットを復元するには、**[ダッシュレット（Dashlet）]** ドロップダウン リストの **[デフォルト セット（Default Set）]** リンクをクリックします。



ストレージ ダッシュボード

[ストレージ（Storage）] ダッシュボードには、SAN および ローカル エリア ネットワーク（LAN）ストレージに関する情報が表示されます。

左のメニュー バーから **[ストレージ（Storage）]** 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 エンクロージャ情報の表示

データソースが構成され、検出が完了すると、検出されたストレージ システムが **[ストレージ エンクロージャ]** 領域の **[名前]** 列の下に表示されます。この領域では、SAN ストレージエンクロージャ、ストレージ システム、またはその両方の詳細を表示できます。

Cisco DCNM Web UI からストレージ エンクロージャ イベント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 **[ダッシュボード > ストレージ（Dashboard > Storage）]**を選択します。

ステップ 2 **[表示]** ドロップダウン リストから、**[SAN ストレージ エンクロージャ]** を選択します。

ステップ 3 詳細を表示するには、ストレージ名を選択します。

イベント、トポロジ、およびトラフィック情報がダッシュボードに表示されます。

ステップ 4 エンクロージャ名を編集するには、ストレージ名を選択して **[名前の変更]** アイコンをクリックします。[エンクロージャーの名前変更] ダイアログ ボックスに新しい名前を入力します。

- 各エンクロージャ名を別の名目に変更できます。エンクロージャ名を選択し、新しい名前を入力して、**[保存]** をクリックします。この手順を繰り返して、必要なすべての必要なエンクロージャ名を変更し、**[適用]** をクリックします。
- すべてのエンクロージャ名を同じ新しい名前に変更できます。**[すべてのメンバーを含める]** チェックボックスをオンにして、新しい名前を入力して、**[適用]** をクリックします。

ステップ 5 **[フィルタ]** アイコンをクリックして、ストレージ エンクロージャを**名前**または **IP アドレス**でフィルタします。

ステップ 6 **[トラフィック]** ペインには、デフォルトで**エンクロージャ トラフィック**が表示されます。**[トラフィック使用率（Traffic Utilization）]** アイコンをクリックして、トラフィック使用率を表示します。エンクロージャ ポートのトラフィック使用率の日次平均パーセンテージが円グラフで表示されます。

円グラフの個々のポート スライスをクリックすると、そのポートの特定のトラフィック使用率の詳細が表示されます。

ストレージ システム情報の表示

Cisco DCNM Web UI からストレージ システムの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 **[ダッシュボード（Dashboard）] > [ストレージ（Storage）]**を選択します。

ステップ 2 **[表示（Show）]** ドロップダウン リストから、**[ストレージ システム（Storage Systems）]** を選択します。

Note
- 検出されたストレージ システムを表示するには、データ ソースを少なくとも 1 回構成および検出する必要があります。
- Cisco DCNM は、検出および表示の点でブロック ストレージとファイラ ストレージを区別するようになりました。ファイラ ストレージには、共有、クォータ、Q ツリーという追加の要素があります。
  - **[共有（Shares）]** : ユーザーがアクセスできるファイル サーバ上の個々のストレージ フォルダ。
  - **[クォータ（Quotas）]** : ファイルとリポジトリのサイズ制限。
  - **[Q ツリー（Q-trees）]** : ツリー ベースのクォータ。Q ツリーを使用すると、データをパーティション分割し、さまざまなバックアップ戦略、セキュリティ スタイル、および設定を利用できます。

ステップ 3 **[クリックして詳細を表示...（Click to see more details...）]** アイコンをクリックして、ストレージ システムの概要を表示します。

[ストレージ システム（Storage Systems）]領域の要素は次のとおりです。

コンポーネント

コンポーネントは、ストレージ システム内のディスクの設定またはサブセットのコンテナです。コンポーネント エレメント 表示には、コレクション内のディスクのテーブルと、管理されているディスクの総数が表示されます。また、コレクションの使用済みスペース対未加工スペースの概要も表示されます。

Procedure

ステップ 1 ストレージ システムドロップダウンを使用して、ストレージ システムを選択します。

ステップ 2 右側のペインには、ストレージコンポーネントの概要が表示されます。各名前をクリックすると、左側のメニューの項目に移動します。

ステップ 3 グラフにマウス カーソルをホバーさせると、その詳細が表示されます。

ステップ 4 左ペインで、詳細を表示するストレージ コンポーネントを選択します。

管理されているディスクの数とその詳細が表示されます。

ステップ 5 シリアル番号をクリックして、ディスクとマッピングされた LUN の詳細を表示します。

ステップ 6 検索ボックスを使用して、特定のコンポーネントを検索できます。

プール

プールは、プール ストレージを表示する LUN のユーザー定義の収集です。プール エレメント ビューには、プールの概要が表示され、プール内の LUN が一覧表示され、管理対象領域と raw 領域の合計も表示されます。

Procedure

ステップ 1 [ストレージ システム（Storage System）] ドロップダウンを使用してストレージ システムを選択します。

各プールの横の棒グラフは、そのプールの総管理スペースを示します。

ステップ 2 左ペインで、表示するプールを選択します。

- プールの状態
- プール内の LUN は、raw 領域の合計と管理対象領域の合計を表示します。
- Raid タイプ
- [ディスクの種類（Disk Type）]
- プール内の LUN の詳細

ステップ 3 検索ボックスを使用して、特定のプールを検索できます。

LUN

LUN は、単一のボリュームに抽象化されたストレージ ボリュームまたはボリュームのコレクションを指します。これは、アクセス保護と管理のためにプールできるストレージの単位です。LUN エレメント ビューの各 LUN は、ホストから LUN へのマッピングとともに表示されます。関連するファブリックも検出されている場合は、ホストと LUN 間のエンドツーエンド接続に関する追加情報も表示されます。

LUN の作成と削除、ホストと LUN マップの作成と削除、HLM のゾーン分割の作成を行うことができます。

Procedure

ステップ 1 [ストレージ システム（Storage System）] ドロップダウンを使用して、ストレージ システムを選択します。

ステップ 2 **[ストレージ（Storage）] > [LUNs]** を選択して、Cisco DCNM から LUN を作成できます。

a) 中央のペインで、**[LUN を追加（Add LUN）]** をクリックします。

b) LUN の有効な**[名前（Name）]**を入力し、その**[タイプ（Type）]**と**[サイズ（Size）]**を選択します。ストレージを切り開いたプールが表示されます。

Note LUN リスト ビューが選択されている場合は、プールの詳細ページから LUN の作成 ポップアップ ウィンドウにアクセスすることもできます。

c) [追加] をクリックします。

確認ウィンドウは全てのステップを表示します。確認後、ステータスは各ステップの結果で更新されます。

LUNの作成が正常に完了したら、ホストの割り当てを行うか、[閉じる]をクリックして、後で [LUN の詳細] ビューからホストを割り当てます。

ステップ 3 詳細を表示するには、左側のナビゲーション ペインで LUN を選択します。

- LUN の詳細と、そのステータスおよび関連ホストの数。
- ホスト LUN マッピングの詳細とアクセス (許可) 情報。

関連するファブリックも検出されている場合は、スイッチインターフェイスと、ホストとLUN間のエンド ツー エンド接続に関するゾーン分割に関する追加情報も表示されます。

Note 検出されたすべてのファブリックはライセンス付与する必要があります。そうでない場合、ファブリックの関連付けはCisco DCNM で無効になっています。この機能を無効にすると、すべての相関フィールドに「ライセンスなしのファブリック（Unlicensed Fabric）」と表示されます。

ステップ 4 SMI-S Storage Enclosure 内の LUN を削除できます。

a) **[ストレージ（Storage）] > [ストレージ システム（Storage System）] > [LUN]** に移動します。

SMI-S Storage Enclosure 内の LUN のリストが右側に表示されます。

b) リストから LUN を 1 つ選択し、**[削除（Remove）]** をクリックします。

確認ウィンドウは全てのステップを表示します。確認後、ステータスは各ステップの結果で更新されます。

c) **[適用 (Apply)]** をクリックします。

ステップ 5 ホストから LUN へのマッピングを追加できます。

a) 左側のペインから **LUN** を選択します。

SMI-S Storage Enclosure 内の LUN のリストが右側に表示されます。

b) 下のリストから LUN を選択します。

そのLUNの現在のホストLUNマッピングを含む、選択したLUNの詳細が表示されます。

c) [追加（Add）] ボタンをクリックします。

[ホストをマスクに追加（Add Hosts to Mask）] ウィンドウが表示されます。

d) 1 つ以上のホストを選択し、**[追加（Add）]** をクリックします。次に、ホストが LUN マッピングに追加されます。さらに、まだゾーニングされていない場合、各 HLM ペアはゾーニングされます。

Note ホスト LUN マッピングは、ホスト ダッシュボードから追加することもできます。詳細については、ホスト ラックの表示, on page 37を参照してください。

ステップ 6 ホストから LUN へのマッピングを削除できます。

a) 左側のペインから **LUN** を選択します。

SMI-S Storage Enclosure 内の LUN のリストが右側に表示されます。

b) 下のリストから LUN を選択します。

その LUN の現在のホスト LUN マッピングを含む、選択した LUN の詳細が表示されます。

c) 1 つ以上の既存のホスト LUN マッピングを選択し、削除アイコンをクリックします。

確認ウィンドウが表示され、各手順が表示されます。

d) **[適用 (Apply)]** をクリックします。

ステータスは各ステップの結果で更新されます。

ステップ 7 (Optional) LUN にゾーニングを追加できます。

a) 左側のペインから **[LUN]** を選択します。

SMI-S Storage Enclosure 内の LUN のリストが右側に表示されます。

b) 下のリストから LUN を選択します。

その LUN の現在のホスト LUN マッピングを含む、選択した LUN の詳細が表示されます。**[ホスト LUN マッピング（Host LUN Mapping）]** テーブルの列の 1 つは、いずれかの HLM が現在ゾーニング用に持っている場合、既存のゾーンを識別します。

c) ゾーニングに「不明」または「なし」の HLM を 1 つ以上選択し、**[ゾーニングの追加（Add Zoning）]** をクリックします。

d) **[適用 (Apply)]** をクリックします。

ステータスは各ステップの結果で更新されます。

ファイラ ボリューム

ファイラ ボリュームは NetApp にのみ適用されます。Filer Volume Element 表示には、ステータス、Containing Aggregate、および合計キャパシティと使用済みスペースが表示されます。

Cisco DCNM Web UI からファイラ ボリュームを表示するには、次の手順を実行します。

Procedure

ステップ 1 ストレージ システム ドロップダウンを使用してストレージ システムを選択します。

ステップ 2 左ペインで、表示するファイラを選択します。

- ファイラの状況と、それを含む集約名。
- グラフにマウス カーソルを置くと、ファイラの合計キャパシティと使用可能なストレージが表示されます。

ステップ 3 検索ボックスを使用して、特定のファイラを検索できます。

ホスト

ホストは、ホストまたはホストエンクロージャに関連付けられたNWWNを、関連付けられたホスト - LUN マッピングおよびホスト ポートとともに記述します。 関連するファブリックも検出されている場合は、ホストと LUN 間の接続に関する追加情報も表示されます。

Cisco DCNM Web UI からホストを構成するには、次の手順を実行します。

Procedure

ステップ 1 [ストレージ システム] ドロップダウンを使用して、ストレージ システムを選択します。

ステップ 2 左ペインで、表示するホストを選択します。

- NWWN（ノード WWN）は、スイッチに接続されているデバイスの WWN です。
- ホスト ポートとホスト LUN マッピング。
- [ホスト ポート（Host Ports）] セクションで、ホスト エンクロージャ名をクリックして、そのイベント、トポロジ、および SAN トラフィックを表示します。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。
- ホスト ポート セクションで、ホスト インターフェイスをクリックして**スイッチ ダッシュボード**を表示します。
- ホスト-LUN マッピング セクションで、ストレージ インターフェイスをクリックしてスイッチ ダッシュボードを表示します。
- [ホスト LUN マッピング（Host-LUN Mapping）] セクションで、ストレージ名をクリックして、そのイベント、トポロジ、および SAN トラフィックを表示します。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。

関連するファブリックも検出されている場合は、スイッチインターフェイスと、ホストとLUN間の接続に関するゾーニングに関する追加情報も表示されます。

Note 検出されたすべてのファブリックはライセンス付与する必要があります。そうでない場合、ファブリックの関連付けは Web UI で無効になっています。この機能を無効にすると、すべての相関フィールドに「ライセンスなしのファブリック（Unlicensed Fabric）」と表示されます。

ステップ 3 検索ボックスを使用して、特定のホストを検索します。

ストレージプロセッサ

ストレージ プロセッサは、ストレージ システム上の要素であり、その機能の一部を有効にします。ストレージ プロセッサには、それが管理するストレージ ポートのコレクションが含まれています。ストレージ プロセッサのエレメント ビューに、ストレージ プロセッサに関連付けられているストレージ ポートのリストが表示されます。

Procedure

ステップ 1 ストレージ システム ドロップダウンを使用してストレージ システムを選択します。

ステップ 2 左ペインで、表示するストレージ プロセッサを選択します。

- ストレージ プロセッサのステータス、アダプタの詳細、およびポートの数。
- ストレージ ポートの詳細。

ステップ 3 検索ボックスを使用して、特定のストレージ プロセッサを検索できます。

ストレージ ポート

ストレージ ポートは、ストレージ システム上の単一のポートです。選択した各ポートの概要情報が表示されます。

Procedure

ステップ 1 [ストレージ システム（Storage System）] ドロップダウンを使用して、ストレージ システムを選択します。

ステップ 2 left ペインで、詳細を表示するためにストレージ ポートを選択します。

ステップ 3 検索ボックスを使用して、特定のストレージ ポートを検索できます。

ストレージ エンクロージャ イベントの表示

Cisco DCNM Web UI からストレージ エンクロージャ イベント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 **[ダッシュボード > ストレージ（Dashboard > Storage）]**を選択します。全て、SAN ストレージ エンクロージャ、またはストレージ システムを選択するためにドロップダウンを使用します。

ストレージ エンクロージャのリストは表に示されています。

ステップ 2 ストレージ エンクロージャの横にある **[イベント（Events）]** アイコンをクリックして、イベント パネルを表示します。

ステップ 3 スライダー コントロールを使用してサイズ変更を行うことができます。

ストレージ エンクロージャ トポロジの表示

Cisco DCNM Web UI からストレージエンクロージャ トポロジ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 **[ダッシュボード > ストレージ（Dashboard > Storage）]**を選択します。全て、SAN ストレージ エンクロージャ、またはストレージ システムを選択するためにドロップダウンを使用します。

テーブルの中にあるストレージ エンクロージャのリストは表示されています。

ステップ 2 行を選択して、トポロジの詳細を表示します。

ステップ 3 マウスのスクロール ホイールを使用して、ズームインおよびズームアウトをします。

ステップ 4 **[ファブリック/ネットワーク（Fabric/Network）]** アイコンをクリックして、ファブリックまたはネットワーク パスを表示します。

ステップ 5 **[すべてのパス（All Paths）]** アイコンをクリックして、完全な設定を表示します。

ステップ 6 **[最短パス（Shortest Path）]** アイコンをクリックして、最初の最短パスを表示します。

Note **[マップ ビュー（Map View）]** アイコンをクリックして、前の手順 4、5、および 6 にリストされているアイコンを有効にします。

ステップ 7 **[表形式のビュー（Tabular View）]** アイコンをクリックして、ホスト トポロジを表形式で表示します。

ストレージ エンクロージャ トラフィックの表示

Cisco DCNM Web UI からストレージ エンクロージャ トラフィックを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[ダッシュボード > ストレージ（Dashboard > Storage）]**を選択します。ドロップダウンを使用して、[すべて（All）]、[SAN ストレージ エンクロージャ（SAN Storage Enclosures）]、または [ストレージ システム（Storage Systems）] を選択します。

ストレージ エンクロージャのリストはテーブルに表示されています。

ステップ 2 行を選択して、トポロジの詳細を表示します。

ステップ 3 ドロップダウンを使用して、期間に応じてトラフィックを選択します。

ステップ 4 アイコンを選択して、トラフィックを**グリッド、折れ線グラフ**、または**積み上げグラフ**として表示します。

ステップ 5 **[イベントの表示（Show Events）]** アイコンをクリックして、イベントを表示します。

ステップ 6 画面下部のオプションを使用して、円グラフまたは折れ線グラフを表示します。チャート上の各名前をクリックすると、その詳細が表示されます。

SAN Insights の導入

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。Cisco DCNM 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。

リリース 11.2(1) からCisco DCNM 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 インサイトの全体的な拡張性を向上させます。

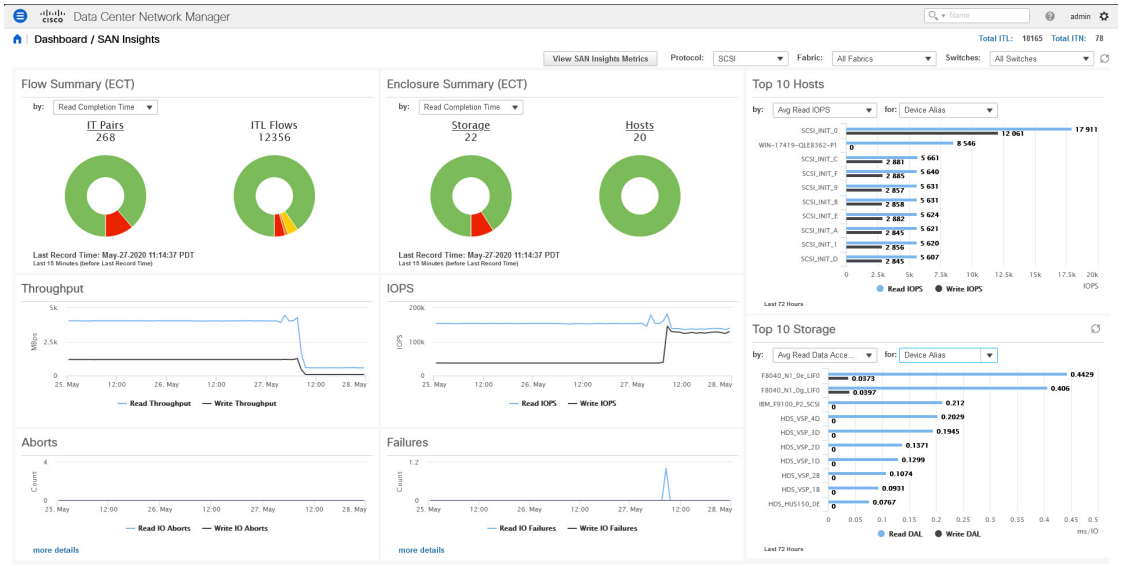
SAN insights ストリーミングの安定性とパフォーマンスのために『*SAN* 展開ガイドの *Cisco DCNM* インストール ガイド』にあるシステム要件セクションと、『*Cisco DCNM SAN* 管理構成ガイド』『』の柔軟な検索データベース ヒープ サイズを増加させるについてのセクションを参照します。システム RAM が十分なサイズであることを確認してください。DCNM とスイッチ間の時刻同期を維持するには、NTP の使用をお勧めします。カウンタ統計を表示するための PM 収集を有効にします。

SAN Insights ダッシュボード

Cisco DCNM 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。

SAN Insights ダッシュボード ページで[プロトコル、ファブリックとスイッチ（protocol, fabric, and switches）]を [protocol, fabric, and switches（プロトコル、ファブリックとスイッチ）] ドロップダウン リストから選択することができます。ダッシュレットには選択した[プロトコル、ファブリックとスイッチ（protocol, fabric, and switches）]についての insight 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。



リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

[ファブリック（Dashboard）] ドロップダウン リストから、SAN Insights のデータとメトリクスを表示する必要がある SAN ファブリックを選択します。ドロップダウン リストに、SAN 分析の機能があり、ライセンスが付与されているスイッチが表示されます。

Note ドーナツの上部にあるタイトルをクリックして、**[モニタ（Monitor）] > [SAN] > [SAN Insights]** の関連ページに移動します。ドーナツのさまざまな色のセクションをクリックして、より詳細なカウントを [パーセンテージ（percentages）]で表示することもできます。

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。

- 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（more details）] をクリックして、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（more details）] をクリックして、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クスに基づいて、選択したプロトコル/ファブリック/スイッチ範囲の上位 10 件のホストエンクロージャ/WWPN[/デバイスエイリアス（Device Alias）]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/WWPN[/デバイス エイリ

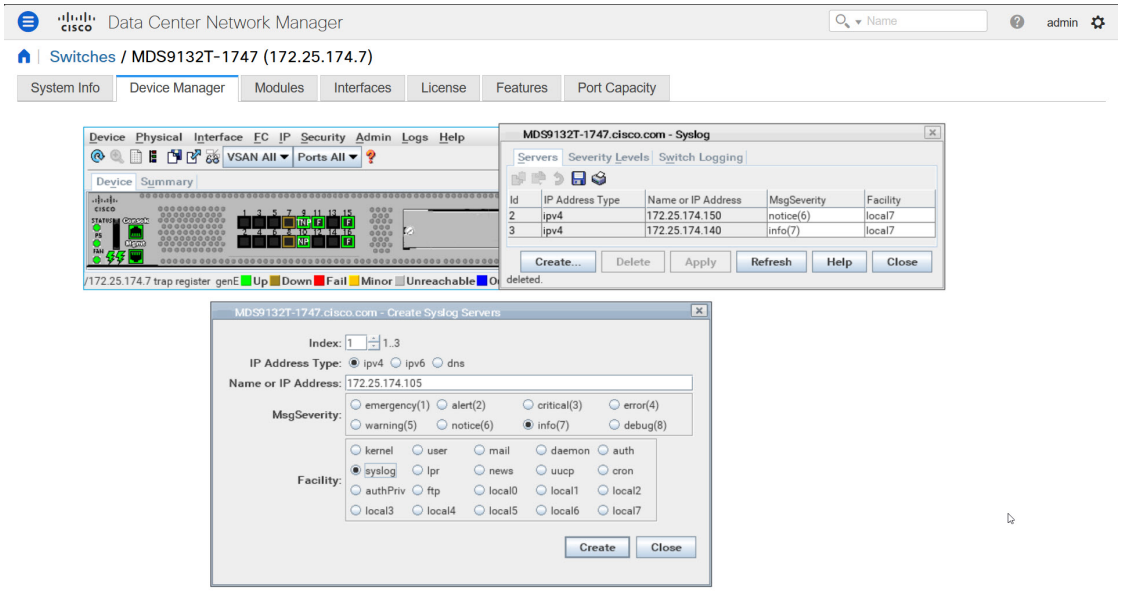
アス（Device Alias）]を表します。データは、読み取り/書き込み IOPS、スループット、Exchange 完了時間、データアクセス遅延でソートできます。

Note 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、DCNM デバイス マネージャで Syslog が構成されていることを確認します。**[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。スイッチをクリックしてシステム情報を表示します。[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、DCNM サーバで 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。

SAN Insights メトリクスの表示

SAN Insights メトリクスを表示するには、**[ダッシュボード（Dashboard）] > [SAN Insights]**を選択します。[SAN Insights Dashboard] ページが表示されます。**[SAN Insights の表示（View SAN Insights Metrics）]** ボタンをクリックします。**[ユース ケース（Use Case）]** ドロップダウン リストから、**[ECT 分析（ECT Analysis）]** または **[カスタム グラフ（Custom Graphing）]** を選択します。

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。

Note ECT 分析とカスタム 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。

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

ECT 分析

Cisco DCNM **[Web UI（）] > [ダッシュボード（）] >]SAN インサイト（）]（Web UI > Dashboard > SAN Insights）]** から、[SAN インサイト メトリックスの表示（View SAN Insights Metrics）] をクリックして ECT 分析を表示します。

ECT 分析には 4 つのコンポーネントがあります。

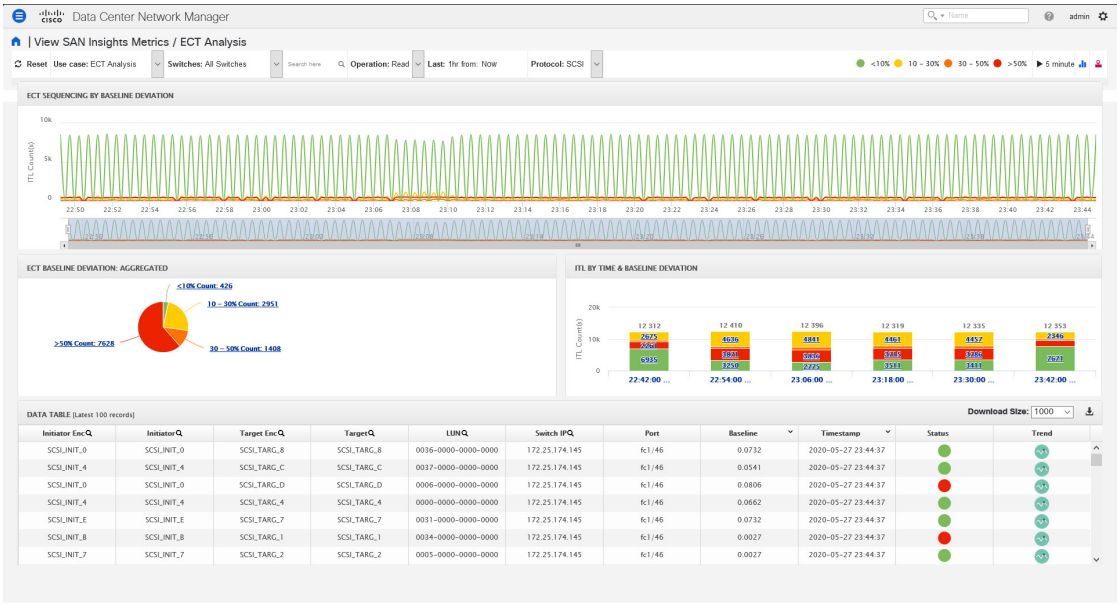
- データ表
- 基準値価格偏差によるECTシーケンシング
- ECT 基準値価格偏差の集計
- 時間および基準値価格偏差による ITL

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロ**

パティ（**Server Properties**）] 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

リリース 11.4(1) 以降、Cisco DCNM では、過去 90 日間の任意の 14 日間のデータを表示できます。(デフォルトの最大 90 日まで)。**[ウェブ UI > 管理 > DCNM サーバー > サーバー プロパティ（Web UI > Administration > DCNM Server > Server Properties）]** で **san.telemetry.expire.rollup** プロパティを変更して、デフォルトの最大日数を変更できます。日付ピッカーを使用して日付を選択し、選択した日付以降の履歴データを時間単位で表示できます。

（注） ECT 分析のデフォルトの期間は 30 分 60 分です。**[リセット]** ボタンをクリックすると、適用されているすべてのデータ フィルタ処理をクリアできます。



（注） **Last** フィルタは、履歴データの期間を表示します。履歴データのデフォルトの期間は 30 分 60 分です。

リリース 11.1(1) から 11.2(1) または 11.3(1) にアップグレードすると、古いデータが期限切れになるまで 2 週間かかります。SAN インサイト メトリックのパフォーマンスは、アップグレードから 2 週間後に向上します。

（注） ECT Analysis ビューのデータは、ドロップダウン リストからスイッチを選択するか、**[ここで検索（Search here）]** フィールドで WWPN\Enclosure Name\LUN-ID\Switch-IP を指定することによってフィルタリングできます。[リリース 11.4(1) 以降では、デバイス エイリアスでフィルタリングすることもできます。（From Release 11.4(1), you can filter it by Device Alias, also.）]

[ここで検索（Search here）] フィールドにテキストを入力して、**[基準値価格偏差による ECT シーケンシング（field to search for the value in the ECT Sequencing by Baseline Deviation）]** テーブルの値を検索できます。

フィルタ処理の **[ここで検索（Search here）]** フィールドは、その値を検索する必要があることを示しています。

ECT 分析ページは、以下のロジックを使用して、現在の正規化された交換完了時間 (ECT) をその履歴の動作 (ECT ベースライン) と比較することにより、ITL フローの集計された動作を表しています。正規化された ECT 値は、KB (KB) のデータを転送するのにかかる時間です。

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（7 days）] 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（14 days）] 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。

（注） 11.4 リリース以降、ECT の偏差が基準値よりも小さい場合、負の偏差と見なされます。Web UI 画面には、計算された偏差パーセンテージに対して負の値が表示されることが想定されます。

リリース 11.4(1) 以降、ECT がベースラインよりも小さいフローは、負の偏差があると識別されます。これは、平均 ECT 偏差に影響を与え、瞬間的なスパイクのシビラティ（重大度）を減らします。ただし、これは ECT パフォーマンスのより良い真の価値を反映しています。

リリース 11.4(1) にアップグレードすると、Web UI の一部のページで古いデータの正しい色が表示されません。2 週間後、新しいデータには適切なカラー コードが表示されます。

（注）

- デフォルトのトレーニング期間を設定するには、Cisco DCNM **[管理（Administration）] > [サーバー プロパティ（Server Properties）]** で `san.telemetry.train.timeframe` パラメータ（デフォルトは 7）を編集します。DCNM サーバ プロセスを再起動します。(Linux で SanInsight サービスを再開するか、SAN-OVA/ISO/SE デプロイメントでポスト プロセッサ アプリを一時停止/再開します)
- 再調整時間を設定するには、Cisco DCNM **[Administration（管理）] > [Server Properties（サーバーのプロパティ）]** で `san.telemetry.train.reset` パラメータ（デフォルトは 14 日）を編集します。DCNM サーバ プロセスを再起動します。Linux で SanInsight サービスを再開するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します。
- たとえば、ベースラインを 4 日間トレーニングし、トレーニング期間の 10 日後にベースラインを再調整するには、トレーニング期間を 4 日に設定し、再調整時間を 14 日に設定します。

表 *2:* 基準値の色の凡例

続柄	値
ECT が基準値から 50% を超える場合	赤
ECT が基準値を超え、30 ～ 50% の範囲にある場合	オレンジ
ECT が基準値を超え、10 ～ 10% の範囲にある場合	イエロー
ECTが基準値から 10% 未満の場合	グリーン（通常を意味します）

ベースライン カラーの凡例の値の範囲は、サーバー プロパティ ファイルで変更できます。**[管理] > [DCNM サーバー] > [サーバー プロパティ]** で **san.telemetry.deviation** の定義を参照してください。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。Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します。

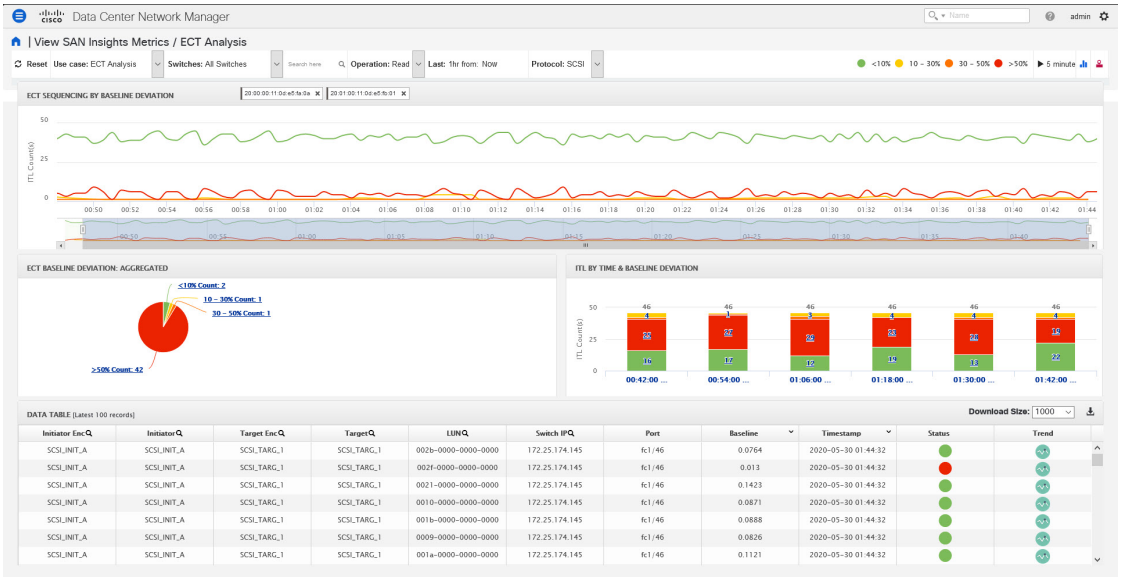
トレンド識別子 ( ) アイコンをクリックして、トレンド識別子に移動できます。詳細については、傾向識別子 （34 ページ）を参照してください。

ECT 分析 UI のデータは、円をクリックして無効または有効にすることで、上記の凡例に対応する ITL のデータを表示するようにフィルタ処理できます。たとえば、黄色とオレンジ色の凡例の円をクリックして無効にすると、対応するデータが表示されます。

データ テーブルの値をコピーして、UI の上部にある **[ここで検索]** 入力フィールドに貼り付けて、すべてのコンポーネントのデータをフィルタ処理できます。データ テーブルの虫眼鏡 ( ) アイコンが付いているすべての列の値は、この機能で検索できる唯一のフィールドです。

ECT BASELINE DEVIATION AGGREGATED（ECT 基準値価格偏差の集計）コンポーネントのデータは、各偏差範囲にある ITL の数を示しています。同様に、ITL BY TIME（時間による ITL）コンポーネントのデータは、各偏差範囲にある時間ごとにグループ化された ITL の数を示します。円グラフまたはヒストグラムのセクションをクリックすると、イニシエータ エンクロージャー、イニシエータ WWPN、ターゲット エンクロージャ、ターゲット WWPN、および LUN/名前空間のドリル ダウン データが表示されます。チャートの対応するセクションをクリックして、結果を .csv 形式でダウンロードします。

（注） ECT 基準値偏差の最大集計データは 20000 に設定されています。



Mozilla ブラウザでのスクリプト タイムアウト エラー

Mozilla ブラウザで、オプションの **[停止]** または **[待機]** でスクリプト タイムアウト エラーが表示された場合は、**[停止]** をクリックしないでください。スクリプト タイムアウト エラーのトラブルシューティングを行うには、次の手順を実行します。

1. Mozilla Firefox を起動します。
2. Firefox のアドレス バーに **about:config** と入力し、Return キーを押します。
3. 確認メッセージで、**[リスクを受け入れます!（I accept the risk!）]** をクリックします。
4. [検索] フィールドに、**dom.max_script_run_time** と入力します。

   基本設定名が表示されます。
5. **dom.max_script_run_time** 基本設定名を右クリックします。

   [変更] を選択します。
6. **dom.max_script_run_time** には、**0** または **20** の整数値を入力します。

7. [OK] をクリックして確定します。
8. Mozilla Firefox ブラウザを再起動します。

カスタムグラフ

これはフリースタイルダッシュボードで、複数のメトリクスを選択でき、選択したメトリクスのリアルタイムデータが[5 minutes（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。

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

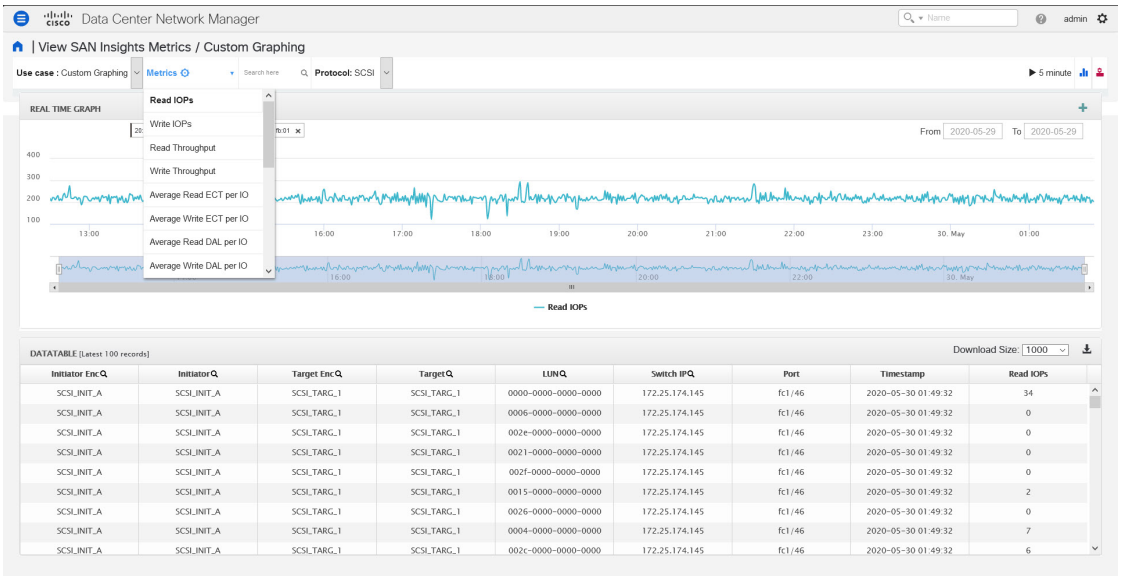
（注） 自動更新オプションはデフォルトで無効になっています。自動更新機能を有効にするには、停止アイコンをクリックする必要があります。

カスタム グラフのユース ケースには 2 つのコンポーネントがあります。

- リアルタイム グラフ
- データテーブル

リアルタイム グラフは、開始日と終了日が選択された対応するメトリクスとともにプロットされます。このコンポーネントには、選択に応じてグラフの下にスライダーが表示されます。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。

11.4 リリースから、Cisco DCNM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。To：日付セレクターを使用して過去の日付を選択し、選択した日付から最大2週間の履歴データを表示します。



リリース 11.4（1）カスタム グラフのメトリクスが拡張され、ドロップダウン メトリクス 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。

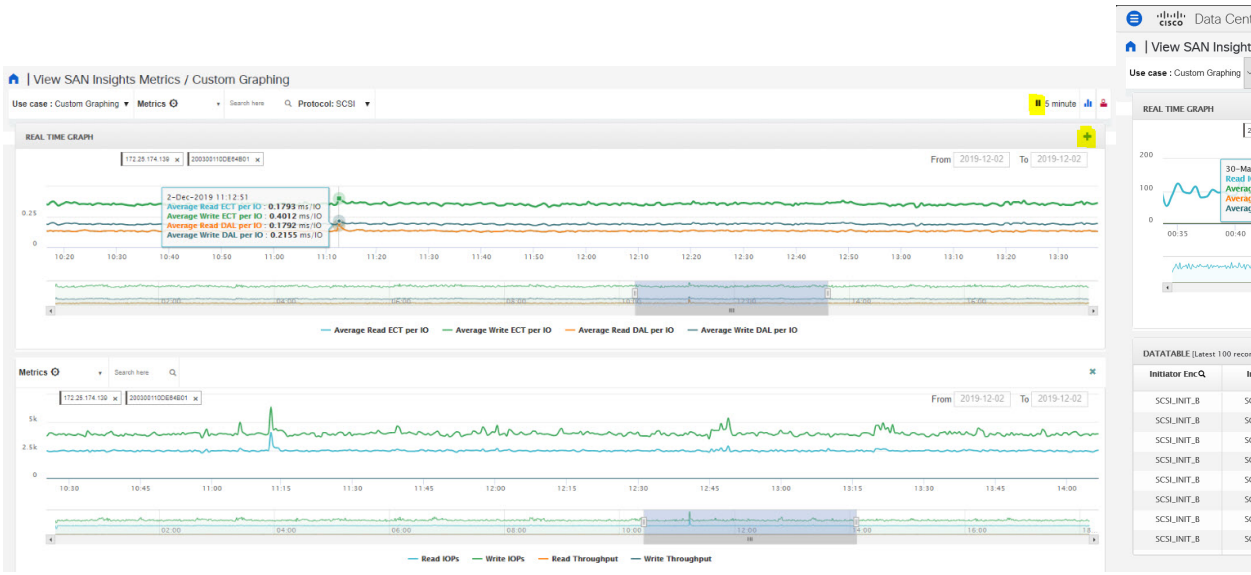
ドロップダウンリストからを失敗またはメトリクスを中止を選択すると、テーブルリストがフィルタ処理され、選択した失敗または中止のメトリクスの少なくとも 1 つをゼロ以外のエントリとして持つ行のみが表示されます。テーブルには 100 レコードのみが表示されます。ただし、ゼロ以外のエラーを見つけやすくするために、テーブルをフィルタ処理して、ゼロ以外の中止または失敗を持つ最後の 100 レコードを表示することができます。失敗または中止を選択すると、テーブルラベルがこの動作を表すように変更されます。

表示するには、検索タブで の [7 つ（seven）]のディメンション (イニシエータ WWN、LUN/NSID、ターゲット WWN、送信元 エンクロージャ、ターゲット エンクロージャ、スイッチ IP[、デバイス エイリアス（, Device Alias）]) のいずれかを入力し、関連するメトリクスを選択します。

右隅にあるダウンロードアイコンをクリックして、データテーブル情報をローカルデータベースにダウンロードして、さらに分析します。

（注） Google Chrome ブラウザを使用して、データテーブル情報をローカル データベースにダウンロードすることをお勧めします。

右上の「＋」アイコン 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。このビューでは、データ テーブルが複数のリアルタイム グラフに置き換えられ、複数選択テキスト検索機能を使用して、プロットする対応するメトリクスを選択できます。

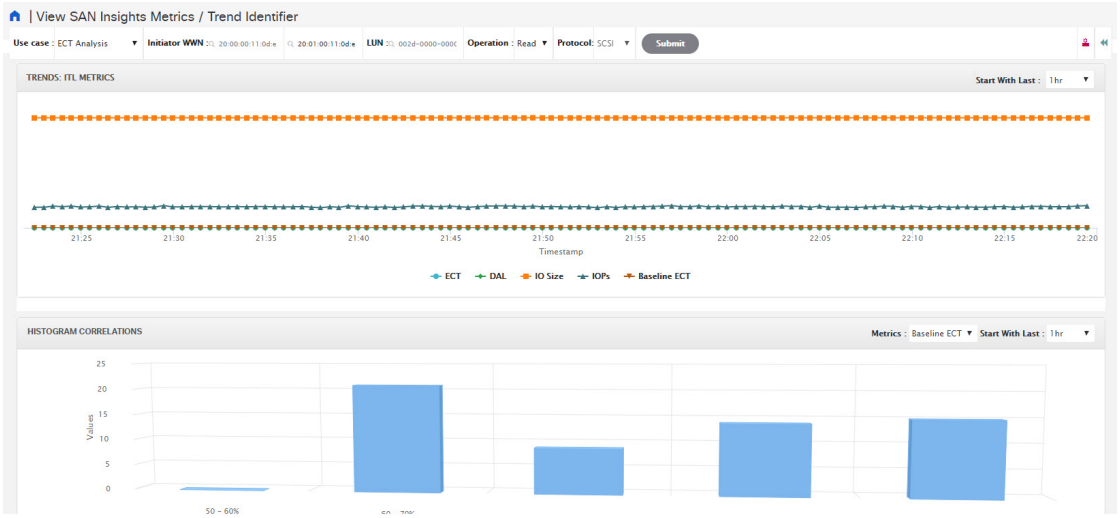


傾向識別子

右上隅の傾向識別子（）アイコンをクリックして、傾向識別子に移動します。

データテーブルの各行にある傾向（）アイコンをクリックして、事前に入力されたITL/ITN入力フィールドを使用して傾向識別子に移動することもできます。選択したITLに対応するデータを示す2つのコンポーネントがあります。傾向ITLメトリクスは、選択した時間間隔（選択した）のECT、DAL、IOサイズ、IOPS、およびベースラインECTの面グラフを示します。[ヒストグラムの相関（Histogram Correlation）]タブには、相関値によってビン化された現在のITLと相関のあるITLの数のヒストグラムが表示されます。このタブのバーをクリックすると、ヒストグラムがデータテーブルに変換され、選択したバーに対応するデータが表示されます。

リリース11.3(1)からCisco DCNM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、**[管理（Administration）]>[DCNMサーバ（DCNM Server）]>[サーバプロパティ（Server Properties）]**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。(LinuxでSanInsightサービスを再起動するか、SAN-OVA/ISO/SE展開でポストプロセッサアプリを一時停止/再開します)



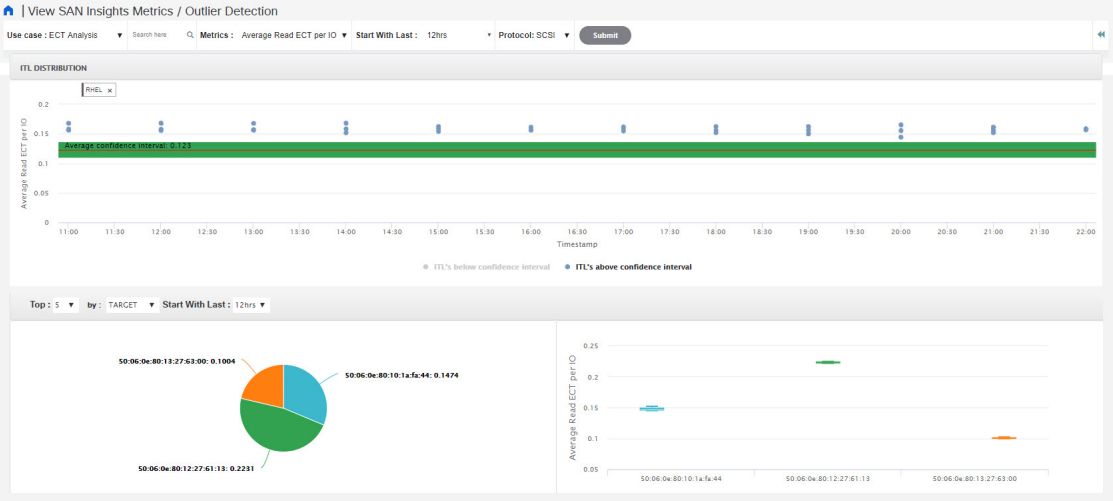
（注） 傾向識別子のデフォルトの間隔は 30 分です。**[Start With Last]** ドロップダウン リストを使用して間隔を指定できます。

外れ値の検出

ページの右上隅に表示される外れ値検出アイコン（ ）をクリックして、**[外れ値検出メトリクス（Outlier Detection）]**を表示します。このページのデータを表示するには、ここで検索入力ボックスにホスト エンクロージャ名またはイニシエータ エンクロージャ名を入力し、メトリクスを選択し、時間範囲を選択して、**[送信（Submit）]**をクリックします。この画面は、60 分ごとに集計データを取得します。

ITL/ITN 分布（ITL/ITN Distribution）タブには、選択した時間間隔（この場合は 1 週間）に存在するすべての ITL/ITN に対して選択されたメトリックの散布図が表示されます。トレンド画面に移動するには、散布図のいずれかのドット (特定の ITL/ITN に対応) をクリックします。機能により、ITL/ITN の 平均以下信頼性間隔と ITL/ITN の 平均以上信頼性間隔の 2 つのタブが追加されました。これら 2 つのタブは、平均信頼性間隔ラインに基づいて計算されたデータです。

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)



マウスをドラッグして表示する特定の領域を選択すると、ズームインして、それぞれのITL/ITNドットをより詳細なレベルで表示できます。ズームされた画面で **[ズームのリセット（Reset Zoom）]** をクリックして、デフォルトのズーム設定を復元します。

このユースケースは、複数選択テキスト検索機能で構成されます。この機能では、任意のフィールド（イニシエータ/ターゲット エンクロージャ）に存在可能な最大 2 つの検索条件で特定のテキストを検索でき、対応するデータが両方のコンポーネントにプロットされます。

Average Confidence Interval は、選択した時間間隔内にほとんどのメトリクス値が含まれる平均線のあるバンドを示します。残りの2つのタブには、選択した時間間隔における選択したメトリックの上位 n (選択された 5 つ) イニシエータ/ターゲットの箱ひげ図と円グラフの分布が表示されます。

ホスト

Note リリース 11.3(1) 以前のリリースでは、この機能は**コンピューティング ダッシュボード**と呼ばれていました。リリース 11.4(1) 以降、名前が**ホスト**に変更されました。

[コンピューティング（Compute）][ホスト（Hosts）] 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（Hosts）]** ダッシュボードは、次の 4 つのパネルで構成されます。

- **[ホスト エンクロージャ（Host Enclosures）]** パネル：ホストおよびネットワーク属性をリストします。

- **[トラフィック（Traffic）]** パネル：I/O 統計情報、CPU およびメモリ情報、個別のホストまたは仮想マシンのディスク遅延を提供します。
- **[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。
- **[イベント（Event）]**パネル：特定のホストエンクロージャ内で構成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。

ここでは、次の内容について説明します。

ホスト ラックの表示

Cisco NX-OS リリース 6.x 以降、Cisco NX-OS デバイスに接続されているネットワーク サーバを表示および検索できます。Cisco DCNM はファブリックの可視性をサーバまで拡張し、ネットワークに接続されているエンド デバイスを検出および検索できるようにします。

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
名前	ホスト名を表示します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを表示します。
#Mac	MAC アドレスの数を表示します。
Mac アドレス	MAC アドレスを表示します。
#WWNs	World Wide Name（WWN）の数を 表示します。
ポート WWN	ポート WWN を表示します。
FCID(s)	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。
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。

フィールド	説明
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 DCNM 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。

Note

- Cisco NX-OS リリース 6.x 以降、サーバ クレデンシャル、サーバ、および静的サーバ アダプタ マッピングは使用できなくなりました。
- Cisco DCNM リリース 10.1 以降、ストレージをホストに割り当てることができます。
- 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。
- DCNM リリース 11.4(1) 以降、デバイス エイリアスからデフォルトのエンクロージャ名を設定できます。**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**[fabric.aliasRE]** プロパティを編集します。

Cisco DCNM 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。

Procedure

ステップ 1 **[ダッシュボード >（Dashboard >）] [ホスト（Host）]** 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 詳細を表示するには、ホストを選択してください。

ダッシュボードのイベント、トポロジ、トラフィック情報が表示されます。ホストエントリの対応するアイコンをクリックして、イベント、トポロジ、およびトラフィック情報を表示することもできます。

DCNM リリース 11.5(1) から、VHost のトラフィック アイコンが追加されました。VHost CPU、メモリ、レイテンシ、ネットワーク I/O などの複数の VM チャートがあります。ホストのラジオ ボタンをクリックして、トラフィック ダッシュボードにそれぞれのトラフィックの詳細を表示します。

ステップ 3 ホスト名を編集するには、行を選択して **[名前の変更（Rename）]** アイコンをクリックします。ポップアップ ダイアログに新しい名前を入力します。

- ホストがポート WWN に関連付けられていない場合、またはエンド ポートが DCNM によって検出されない場合、それは VHost または LAN ホストです。**[エンクロージャの名前を変更（Rename Enclosure）]** ダイアログ ボックスは、既存の名前に対してのみ表示されます。
- ホストがポート WWN に関連付けられていて、エンド ポートが DCNM によって検出されている場合。関連付けられたホスト名の **[エンクロージャの名前を変更（Rename Enclosure）]** ダイアログが表示されます。
  - 各エンクロージャ名を別の名目に変更できます。エンクロージャ名を選択し、新しい名前を入力して、[保存（Save）] をクリックします。この手順を繰り返して、必要なすべてのエンクロージャ名を変更し、**[適用（Apply）]** をクリックします。
  - すべてのエンクロージャ名を同じ新しい名前に変更できます。**[すべてのメンバーを含める（Include All Members）]** チェック ボックスをオンにし、新しい名前を入力して、**[適用（Apply）]** をクリックします。

Note 空白の名前を指定すると、サーバはその名前をデフォルトにします。

Cisco DCNM では、デフォルトの割り当てられたホスト エンクロージャ名を変更したり、同じ名前を割り当てることで複数のエンクロージャを同じエンクロージャにグループ化したりできます。それぞれの WWPN へのカスタム エンクロージャ名の割り当ては、Cisco DCNM SAN クライアントでのみサポートされています。

ステップ 4 ストレージをホストに割り当てるには、ホストを選択し、[名前の変更（Rename）]アイコンの横にある **[割り当て（Assign）]** アイコンをクリックします。

[ストレージをホストに割り当て（Assign Storage to Host）] ウィンドウが表示されます。ホストの選択はエンクロージャ単位で、LUNの複数選択が可能です。[指定する（Assign）]をクリックします。確認用のメッセージが表示されます。確認後、ステータスは各ステップの結果で更新されます。

ステップ 5 **[クイック フィルタ]** ドロップダウンをクリックして、**LAN**、**SAN**、および**仮想**によって**ホスト** エンクロージャ（ストレージではない）をフィルタ処理します。

ホスト イベントの表示

Cisco DCNM Web UI からホスト イベントを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[ダッシュボード >（Dashboard >）] [ホスト（Host）]** 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 エンクロージャの横にある **[イベント（Events）]** アイコンをクリックして、イベント パネルを表示します。

スライダー コントロールを使用してサイズ変更を行うことができます。

ホスト トポロジの表示

Cisco DCNM Web UI からホスト トポロジを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[ダッシュボード >（Dashboard >）] [ホスト（Host）]** 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 行を選択して、ホスト トポロジの詳細を表示します。

マウスのスクロール ホイールを使用して、ズームインおよびズームアウトができます。

ステップ 3 **[ファブリック/ネットワーク（Fabric/Network）]** アイコンをクリックして、ファブリックとネットワーク パスを表示します。

1 - ファブリック/ネットワーク

2 - すべてのパス

3 - 最初の最短経路

4 - マップ ビュー

5 - 表形式のビュー

6 - カスタム ポート グループ

7 - ズームイン

8 - ズームアウト

9 -ウィンドウに合わせる

ステップ 4 **[すべてのパス（All Paths）]** アイコンをクリックして、完全な設定を表示します。

ステップ 5 **[最初の最短パス（First Shortest Path）]** アイコンをクリックして、最初の最短パスを表示します。

Note **[マップ ビュー（Map View）]** アイコンをクリックして、前の手順 4、5、および 6 にリストされているアイコンを有効にします。

ステップ 6 **[表形式のビュー（Tabular View）]** アイコンをクリックして、ホスト トポロジを表形式で表示します。

ステップ 7 **[カスタム ポート グループ（Custom Port Group）]** アイコンをクリックして、カスタム ポート グループを表示します。

ホスト トラフィックの表示

Cisco DCNM ウェブ UI からホスト トラフィックを表示するには、次の手順を実行します。

Procedure

ステップ 1 メニュー バーで、**[ダッシュボード >（Dashboard >）][ホスト（Hosts）]**の順に選択します。

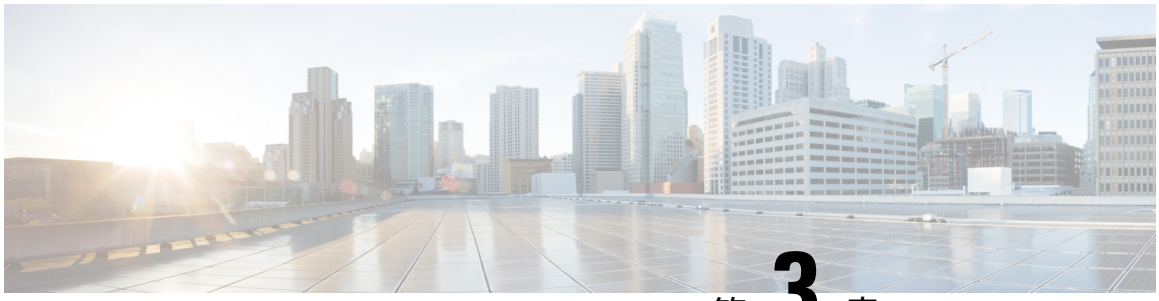
ホスト エンクロージャ テーブルのホストのリストが表示されます。

ステップ 2 行を選択して、ホスト トポロジの詳細を表示します。

ステップ 3 ドロップダウンを使用して、期間に応じてトラフィックを選択します。

ステップ 4 アイコンを選択して、トラフィックを**グリッド、折れ線グラフ**、あるいは、**積み上げグラフ**として表示します。

ステップ 5 **[トラフィック（Traffic）]** ペインには、デフォルトで**[エンクロージャ トラフィック（Enclosure Traffic）]**が表示されます。**[トラフィック使用率（Traffic Utilization）]** アイコンをクリックして、トラフィック使用率を表示します。エンクロージャ ポートのトラフィック使用率の日次平均パーセンテージが円グラフで表示されます。



第 3 章

トポロジ

トポロジ

[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ホバーさせます。また、リンクのノードまたは線をクリックします。ウィンドウの右側からスライドインペインが表示されます。このペインには、スイッチまたはリンクに関する詳細情報が表示されます。

Note 複数のタブを同時に開いたり、並べて機能させたりして、比較やトラブルシューティングをすることができます。

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。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。

Note

- **[トポロジ（Topology）]** ウィンドウでは、FEX の正常性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。ポートの移動は、**[トポロジ（Topology）]** ウィンドウでは更新されません。更新されたポートが DCNM に表示されるようにスイッチを再検出する必要があります。

- 黒：エレメントがダウンしていることを示します。

Cisco DCNM リリース 11.4(1) 以降、スイッチがメンテナンス モードの場合、スイッチの横に **メンテナンス モード バッジ**が表示されます。スイッチが移行モードの場合、スイッチの横に **移行モード**のバッジが表示されます。

スコープ

範囲に基づいてトポロジを検索できます。**[範囲（SCOPE）]** ドロップダウン リストから使用可能なデフォルトの範囲は、**[DEFAULT_LAN]** および **[DEFAULT_SAN]** です。検索オプションは、選択した範囲によって異なります。

[DEFAULT_LAN] では、次の検索オプションを使用できます。

- 高速検索
- VLAN

[DEFAULT_SAN] では、次の検索オプションを使用できます。

- 高速検索
- VLAN
- VSAN ID/名前

検索

ノード数が多いと、目的のスイッチやリンクを見つけるのがすぐに難しくなります。検索を実行すると、スイッチやリンクをすばやく見つけることができます。VM トラッカーと汎用セットアップを検索することもできます。検索機能により、ホストが接続されているリーフを確認できます。

次の検索が利用できます。

Note デフォルトでは、クイック検索が選択されています。

高速検索

[高速検索（Quick Search）] では、名前、IP アドレス、モデル、シリアル番号、スイッチの役割でデバイスを検索できます。**[検索（Search）]** フィールドに検索パラメータを入力すると、トポロジ内で対応するスイッチが強調表示されます。複数のノードおよびリンクの検索を実行するには、複数のキーワードをコンマで区切ります（例：ABCD12345、N7K、sw-dc4-12345, core、172.23.45.67）。Cisco DCNM はワイルドカード検索もサポートしています。シリアル番号またはスイッチ名の一部がわかっている場合は、ABCD*、sw*12345、core などのように、アスタリスクを付けてこれらの部分的な用語で検索を構築できます。

検索の範囲をパラメータに制限するには、パラメータ名の後にスペースを入力し、パラメータを [検索（Search）] フィールドに入力します（例：name=sw*12345、serialNumber=ABCD12345 など）。

VLAN

指定された VLAN ID で検索します。VLAN 検索では、スイッチまたはリンクに構成されている VLAN を検索できます。STP が有効になっている場合、STP プロトコルに関連する情報とリンクの STP 情報が提供されます。

VSAN ID/名前

指定された VSAN ID で検索します。VSAN 検索では、スイッチまたはリンクに設定されている VSAN を検索できます。VSAN に関連付けられた STP の詳細を表示するには、**[STP の詳細（STP Details）]** リンクをクリックします。

STP が有効になっている場合、STP の詳細が表示されます。リンクがブロックされている場合、リンクは赤、転送リンクの場合は緑、リンクが 1 つの VSAN 範囲でブロックされ、別の VSAN 範囲の転送がブロックされている場合はオレンジでマークされます。

この検索は、デフォルトの LAN 範囲と SAN 範囲の両方に適用できます。

パネルを表示

次のオプションに基づいてトポロジを表示することを選択できます。

- **[自動更新（Auto Refresh）**：このチェック ボックスをオンにすると、トポロジが自動的に更新されます。
- **[スイッチの正常性（Switch Health）]**：このチェックボックスをオンにして、スイッチの健全性ステータスを表示します。
- **FEX**：このチェックボックスをオンにして、ファブリック エクステンダを表示します。

Note FEX 機能は、ローカル エリア ネットワーク（LAN）デバイスでのみ使用できます。したがって、このチェックボックスをオンにすると、FEX をサポートする Cisco Nexus スイッチのみが表示されます。

Note [Cisco Nexus スイッチが SAN ファブリックの一部として検出された場合、FEX 機能は使用できません。（If a Cisco Nexus Switch is discovered as part of SAN fabric, FEX feature is not available.）] FEX は、Cisco Nexus 1000V デバイスでもサポートされていません。したがって、**[FEX]** チェックボックスをオンにしても、そのようなデバイスはトポロジに表示されません。

- **[リンク（Links）]**：このチェックボックスを選択し、トポロジのリンクを表示します。次のオプションを使用できます。
  - **[エラーのみ（Errors Only）]**：エラーのあるリンクのみを表示するには、このラジオボタンをクリックします。
  - **[すべて（All）]**：このラジオボタンをクリックして、トポロジ内のすべてのリンクを表示します。
  - **[VPC のみ（VPC Only）]**：vPC ピア リンクと vPC のみを表示するには、このチェックボックスをオンにします。
  - **[帯域幅（Bandwidth）]**：リンクによって消費される帯域幅に基づいて色分けを表示するには、このチェック ボックスをオンにします。
- **[UI 制御（UI controls）]**：チェック ボックスをオンにして、**[トポロジ（Topology）]** ウィンドウのさまざまな制御を表示または非表示にします。
- **[更新（Refresh）]**：このパネルの右上隅にある **[更新（Refresh）]** アイコンをクリックして、トポロジの更新を実行することもできます。

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、DCNM は 16 のスイッチごとにリーフ層を分割します。

- **[ランダム（Random）]**: ノードはウィンドウ上に[ランダム（randomly）]に配置されます。DCNM 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。
- **[円形（Circular）]** および **[同心円状（Tiered-Circular）]**：ノードを円形または同心円状に描画します。
- **[カスタム保存レイアウト（Custom saved layout）]**：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、DCNM 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、DCNM 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、DCNM それを使用します。カスタム レイアウトが適用されていない場合は、DCNM 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。

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。

スイッチ スライドアウト パネル

構成したスイッチ名、IP アドレス、スイッチ モデルとステーテス、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要約情報をスイッチをクリックすることで表示することができます。

DCNM リリース 11.5（1）からスイッチの役割は、コア ルータとエッジ ルータの 2 つだけです。

ビーコン

このボタンは、**beacon** コマンドをサポートするスイッチに表示されます。ビーコンが開始されると、ボタンにカウントダウンが表示されます。デフォルトでは、ビーコンは 60 秒後に停止しますが、**[ビーコンの停止（Stop Beacon）]** をクリックしてすぐに停止できます。

Note デフォルト時間は、`server.properties` ファイルで構成できます。**beacon.turnOff.time** を検索します。ミリ秒単位の時間。この機能を有効にするには、サーバの再起動が必要です。

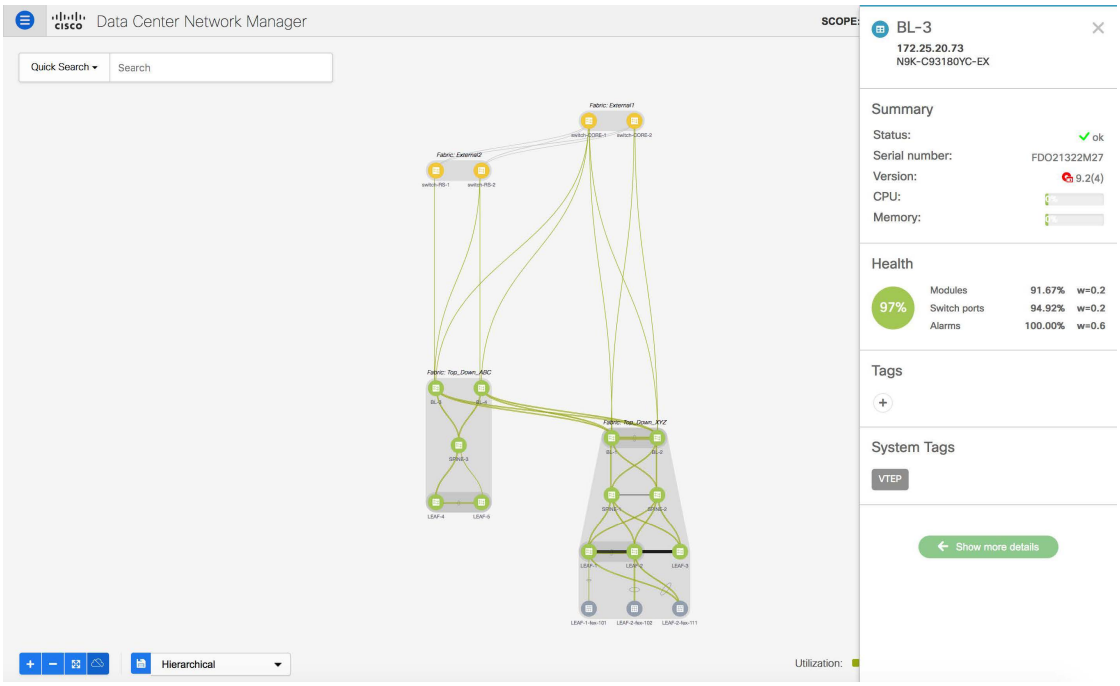
タギング

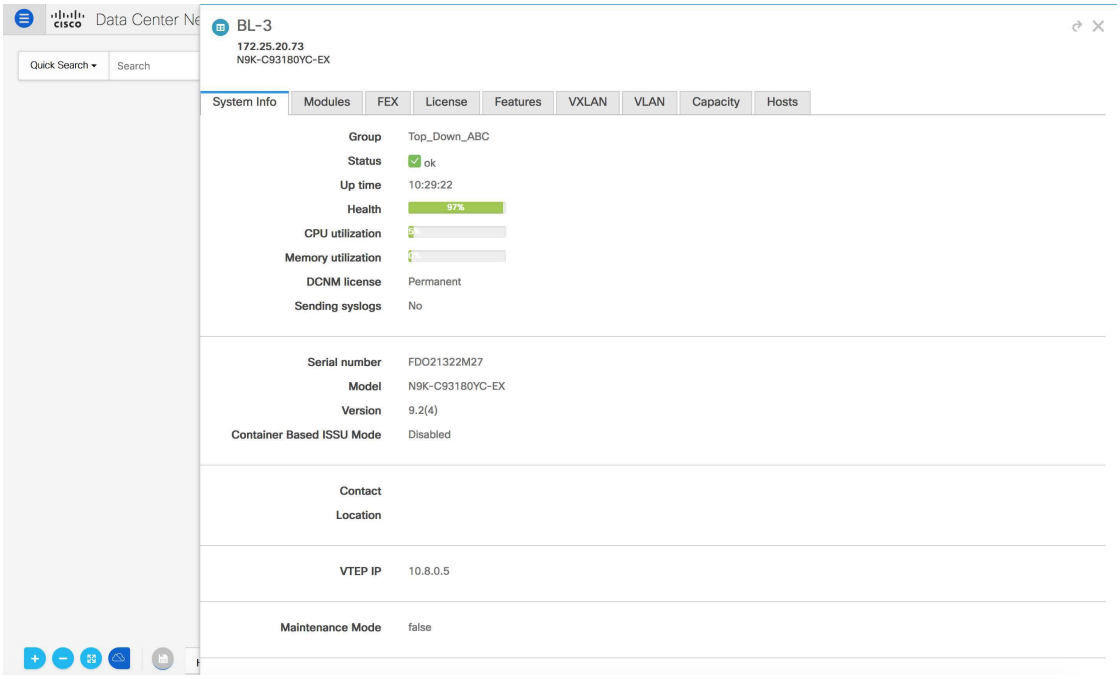
タグ付けは、スイッチを整理するための強力かつ簡単な方法です。タグは、*[建物 6（building 6）]*、*[フロア 2（floor 2）]*、*[ラック 7（rack 7）]*、*[問題スイッチ（problem switch）]*、*[ジャスティン デバッグ（Justin debugging）]* など、事実上任意の文字列にすることができます。

検索機能を使用して、タグに基づいて検索を実行します。

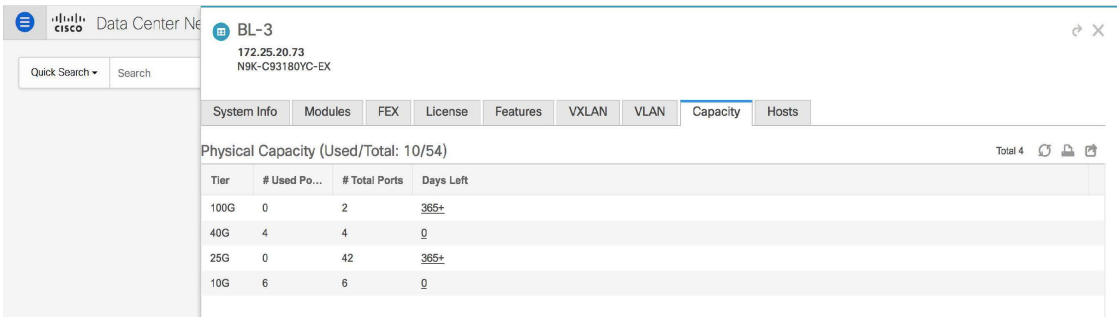
詳細の表示

[詳細を表示（Show more details）] をクリックして、**[システム情報、モジュール、FEX、ライセンス、機能、VXLAN、VLAN、容量（System Info, Modules, FEX, License, Features, VXLAN, VLAN, Capacity）]**、および **[ホスト（Host）]** のタブの下に詳細情報を表示します。





Cisco DCNM リリース 11.4(1) 以降、400G 層も **[キャパシティ（Capacity）]** タブの **[物理キャパシティ（Physical Capacity）]** テーブルに追加されています。ただし、**[キャパシティ（Capacity）]** タブの **[物理キャパシティ（Physical Capacity）]** テーブルには、スイッチに存在する物理ポートに関する情報のみが表示されます。たとえば、スイッチに 400G の物理ポートがない場合、400G 層は、**[物理キャパシティ（Physical Capacity）]** テーブルに表示されません。

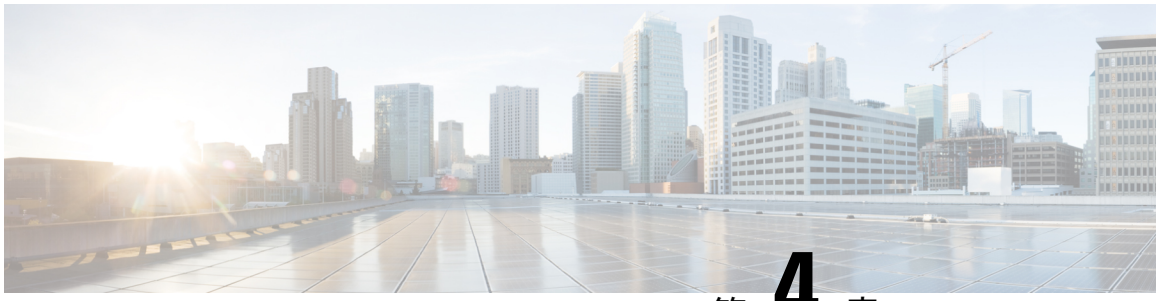


リンク スライドアウト パネル

リンクをクリックして、ステータスと、リンクを説明するポートまたはスイッチを表示できます。

24 時間トラフィック

この機能を使用するには、**パフォーマンス モニタリング**を**オン**にする必要があります。**[パフォーマンス監視（Performance Monitoring）]** が **[オン（ON）]** になると、トラフィック情報が収集され、集約情報がグラフ トラフィックの使用状況とともに表示されます。



第 4 章

インベントリ

この章は次のトピックで構成されています。

インベントリ情報の表示

Cisco DCNM リリース 6.x 以降では、グローバル範囲 ペインを使用して、SAN スイッチとローカル エリア ネットワーク（LAN）スイッチの両方のインベントリとパフォーマンスを表示できます。インベントリ情報を表示するには、ローカル エリア ネットワーク（LAN）、SAN、またはその両方を選択できます。インベントリ情報をエクスポートして印刷することもできます。

この情報を印刷またはMicrosoft Excel にエクスポートすることができます。

Note **[印刷（Print）]** アイコンを使用して表示されている情報を印刷するか、**[エクスポート（Export）]** アイコンを使用して表示されている情報を Microsoft Excel スプレッドシートにエクスポートすることもできます。表示する列を選択することもできます。

[Inventory] メニューには、次のサブメニューがあります。

スイッチのインベントリ情報の表示

Cisco DCNM Web UI のスイッチ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 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** を選択します。

[スイッチ（Switches）] ウィンドウが選択した [範囲（Scope）] のすべてのスイッチのリストともに表示されます。

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、スイッチが属するスイッチ グループが表示されます。
- **[デバイス名（Device Name）]** 列でスイッチを選択して、スイッチ ダッシュボードを表示します。
- **[IP アドレス]** 列にはスイッチの IP アドレスを表示します。
- **[WWN/シャーシ ID（WWN/Chassis ID）]** には、ワールドワイド名（WWN）がある場合、またはシャーシ ID が表示されます。
- **[正常性（Health）]** には、スイッチの正常性の状況が表示されます。

  Note Cisco DCNM 上のすべてのスイッチの最新の正常性データを更新して再計算するには、スイッチ テーブルの上にある **[正常性の再計算（Recalculate Health）]** ボタンをクリックします。

- **[モード]**列には、スイッチの現在のモードを指定します。スイッチは、**通常**、**メンテナンス**、または**移行**モードにすることができます。
- **[ステータス（Status）]** 列には、スイッチのステータスが表示されます。
- **[# ポート（#Ports）]** 列には、ポートの数が表示されます。
- **[モデル（Model）]** 列には、スイッチのモデル名が表示されます。
- **[シリアル番号（Serial No.）]** 列には、スイッチのシリアル番号を表示します。
- **[リリース（Release）]** 列には、スイッチのバージョンが表示されます。
- **[稼働時間（Up Time）]**列には、スイッチがアクティブになっている時間が表示されます。
- **[コンテナベースの ISSU モード（Container Based ISSU Mode）]** 列は、コンテナベースの ISSU モードが有効かどうかを示します。コンテナ ベースの ISSU は、Cisco Nexus 3000 および Cisco Nexus 9000 シリーズ スイッチで有効にできます。これは、デバイスでの 1 回限りの構成です。

  拡張インサービス ソフトウェア アップグレード（ISSU）：スイッチがトラフィックを転送し続けている間にデバイス ソフトウェアをアップグレードできます。これにより、ソフトウェア アップグレードによって通常発生するダウンタイムが削減されます（通常の ISSU に似ており、無停止アップグレードとも呼ばれます）。 ただし、コンテナベースの ISSU を使用すると、ソフトウェアは、個別の Linux コンテナ（LXC）内で、スーパーバイザおよびライン カードに対して実行され、3 番目のコンテナが ISSU 手順の一部として作成され、スタンバイ スーパバイザとして起動されます。

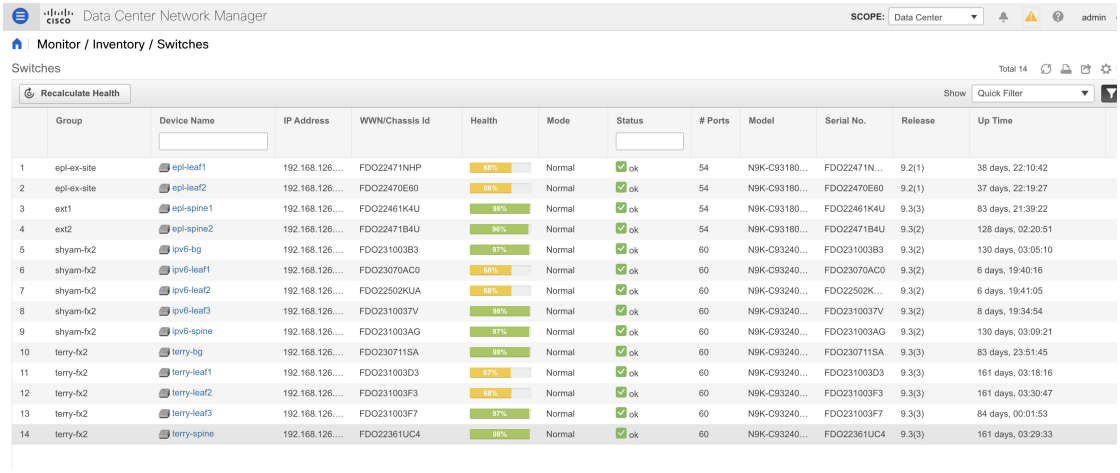
  コンテナ ベースの ISSU は、Cisco Nexus 3164Q、9200 シリーズ スイッチ、9332PQ、9372PX、9372TX、9396PX、9396TX、93120TX、および 93128TX スイッチでサポートされています。

  コンテナ ベースの ISSU 機能がサポートされている Cisco Nexus 3000 および 9000 スイッチの詳細については、次の URL を参照してください。

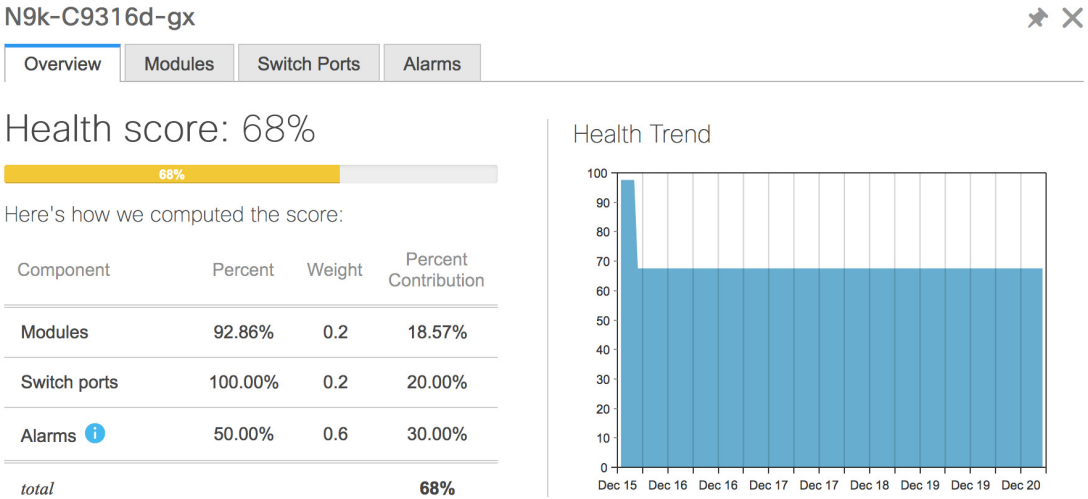
Cisco Nexus 9000 シリーズ NX-OS リリース 9.x ソフトウェア アップグレード/ダウングレード ガイド

Cisco Nexus 3000 シリーズ NX-OS ソフトウェア アップグレード/ダウングレード ガイド、リリース 9.x

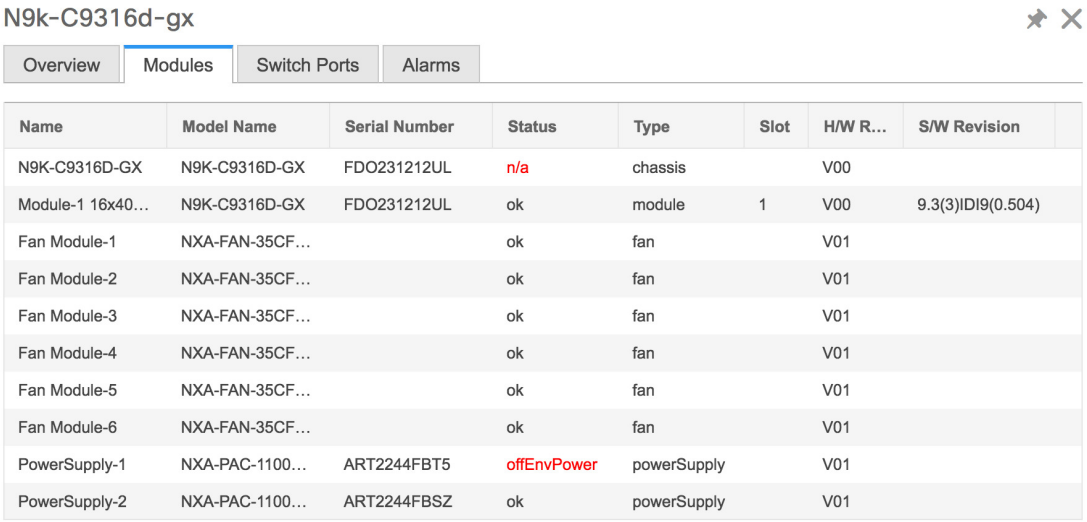
Cisco NX-OS ISSU サポート マトリクス



ステップ 3 **[正常性（Health）]** をクリックして、デバイスの [正常性スコア（Health）] ウィンドウにアクセスします。[正常性スコア（Health score）] ウィンドウには、正常性スコアの計算と正常性トレンドが含まれています。[概要（Overview）] タブには、全体的な正常性スコアが表示されます。正常性スコアの計算時には、すべてのモジュール、スイッチ ポート、およびアラームが考慮されます。特定の日付の詳細情報については、[正常性トレンド（Health Trend ）] の下のグラフにカーソルを合わせます。[アラーム（Health score）] の横にある情報アイコンにカーソルを合わせると、生成された重大、メジャー、マイナー、および警告のアラームの数が表示されます。

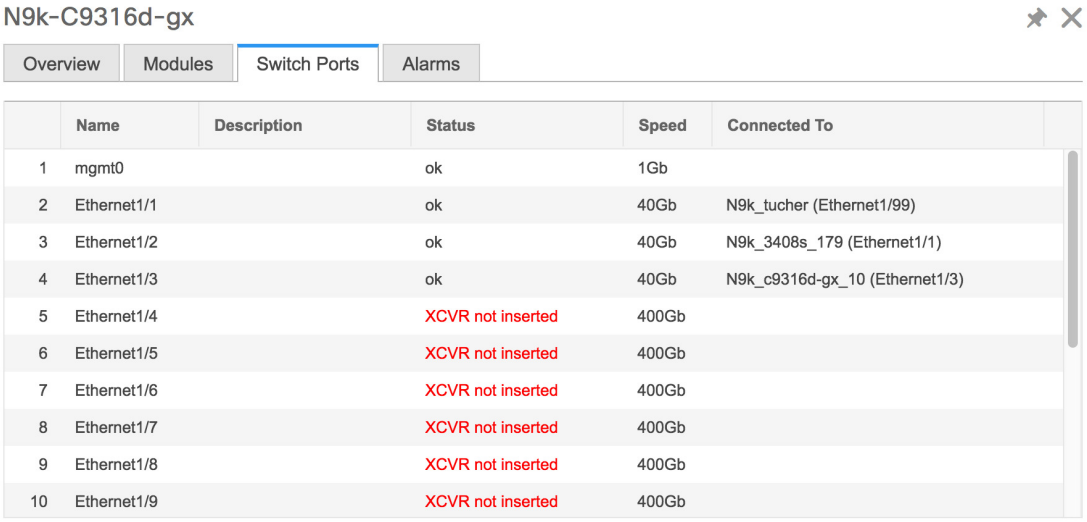


[モジュール（Modules）] タブをクリックして、デバイスのさまざまなモジュールに関する情報を表示します。このタブには、名前、モデル名、シリアル番号、ステータス、タイプ、スロット、ハードウェア リビジョン、ソフトウェア リビジョンなどの情報が表示されます。



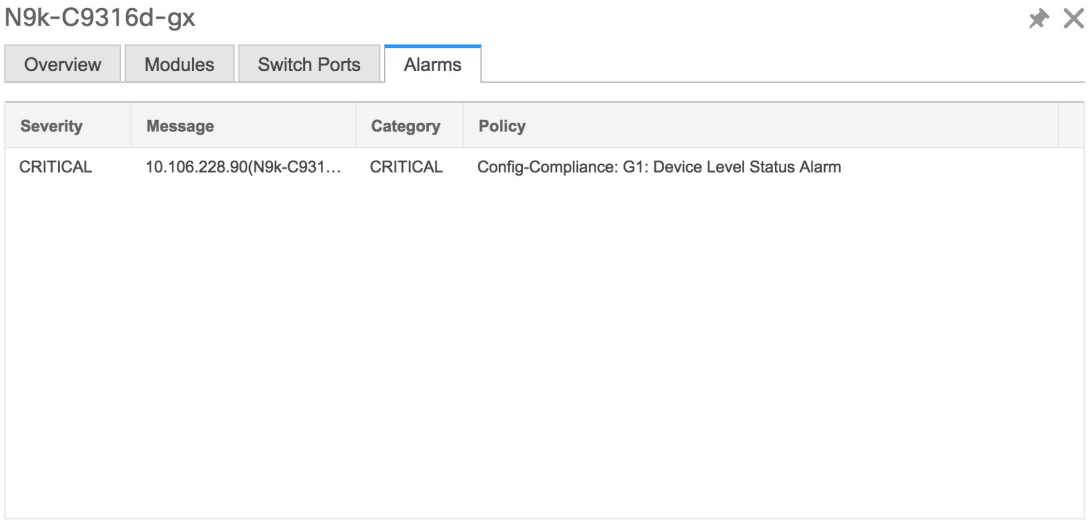
Name	Model Name	Serial Number	Status	Type	Slot	H/W R...	S/W Revision
N9K-C9316D-GX	N9K-C9316D-GX	FDO231212UL	n/a	chassis		V00	
Module-1 16x40...	N9K-C9316D-GX	FDO231212UL	ok	module	1	V00	9.3(3)IDI9(0.504)
Fan Module-1	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-2	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-3	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-4	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-5	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-6	NXA-FAN-35CF...		ok	fan		V01	
PowerSupply-1	NXA-PAC-1100...	ART2244FBT5	offEnvPower	powerSupply		V01	
PowerSupply-2	NXA-PAC-1100...	ART2244FBSZ	ok	powerSupply		V01	

[スイッチ ポート（Switch Ports）] タブをクリックして、デバイス ポートに関する情報を表示します。このタブには、名前、説明、ステータス、速度、ポートが接続されているデバイスなどの情報が表示されます。



	Name	Description	Status	Speed	Connected To
1	mgmt0		ok	1Gb	
2	Ethernet1/1		ok	40Gb	N9k_tucher (Ethernet1/99)
3	Ethernet1/2		ok	40Gb	N9k_3408s_179 (Ethernet1/1)
4	Ethernet1/3		ok	40Gb	N9k_c9316d-gx_10 (Ethernet1/3)
5	Ethernet1/4		XCVR not inserted	400Gb	
6	Ethernet1/5		XCVR not inserted	400Gb	
7	Ethernet1/6		XCVR not inserted	400Gb	
8	Ethernet1/7		XCVR not inserted	400Gb	
9	Ethernet1/8		XCVR not inserted	400Gb	
10	Ethernet1/9		XCVR not inserted	400Gb	

[アラーム（Alarm）] タブをクリックして、生成されたアラームに関する情報を表示します。このタブには、アラームの重大度、メッセージ、カテゴリ、およびアラームが生成されたためにアクティブ化されたポリシーなどの情報が表示されます。



[正常性（Health）] 列では、スイッチの正常性は、次のパラメーターに基づいてキャパシティ マネージャーによって計算されます。

- モジュールの合計数
- 警告の影響を受けたモジュールの総数
- スイッチ ポートの合計数
- 警告の影響を受けたスイッチ ポートの総数
- シビラティがクリティカルのアラームの総数
- シビラティが警告のアラームの総数
- 重大度の重大なアラームの総数
- 重大度が小さいアラームの総数

ステップ 4 **[正常性（Health）]** 列の値は、以下に基づいて計算されます。

- 警告の影響を受けるモジュールの割合（正常性全体の 20% に寄与）。
- 警告の影響を受けるポートの割合（正常性全体の 20% に影響します）。
- アラームのパーセンテージ（正常性全体の 60% に影響します）。このパーセンテージの最大値を占めるのはクリティカル アラームで、次にメジャー アラーム、マイナー アラーム、および警告アラームが続きます。

共通インターフェイス クラス com.cisco.dcbu.sm.common.rif.HealthCalculatorRif を実装して、独自の正常性計算式を持つこともできます。

デフォルトの Java クラスは health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculatorAlarms として定義されています。

- Capacity Manager は、ライセンス スイッチの正常性のみを計算します。正常性カラムに値が表示されない場合は、スイッチにライセンスがないか、キャパシティ マネージャの毎日のサイクルを実行できていません。
- スイッチにライセンスがない場合は、[DCNM License] 列で**[ライセンスなし（Unlicensed）]** をクリックします。**[管理（Administration）] > [ライセンス（License）]** ウィンドウが表示され、ユーザーにライセンスを割り当てることができます。
- キャパシティ マネージャは、DCNM サーバーが起動してから 2 時間後に実行されます。したがって、DCNM 開始時刻の 2 時間後にデバイスを検出した場合、正常性はこの DCNM 開始時刻の 24 時間後に計算されます。

Cisco DCNM 11.3(1) リリース以降では、**[トポロジ（Topology）]** ウィンドウでスイッチをクリックするか、**[制御（Control）]>[ファブリック（Fabrics）]>[ファブリック ビルダー（Fabric Builder）]** を選択し、ファブリックを選択してから**ファブリック ビルダー** ウィンドウのスイッチをクリックすることにより、スイッチの概要とともにスイッチの状態に関する情報を表示できます。

システム情報の表示

スイッチのダッシュボードには、選択したスイッチの詳細が表示されます。

Procedure

ステップ 1 Cisco DCNM ホームページから、**[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** を選択します。

Cisco DCNM Web UI によって検出されたすべてのスイッチのインベントリが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列のスイッチをクリックします。

そのスイッチに対応する**スイッチ** ダッシュボードが、次の情報とともに表示されます。

ステップ 3 **[システム情報（System Info）]** タブをクリックします。このタブには、グループ名、ヘルス、モジュール、システムが稼働している時間、シリアル番号、バージョン番号、連絡先、場所、DCNM ライセンス、ステータス、システム ログ送信ステータス、CPU とメモリの使用率、VTEP IP などの詳細なシステム情報が表示されます。アドレスが表示されます。**[正常性]** をクリックして、正常性スコアの計算と正常性トレンドを含む [正常性スコア] 画面にアクセスします。 ポップアップには、概要、モジュール、スイッチ ポート、イベント タブが含まれています。

- （オプション）**SSH** をクリックして、Secure Shell（SSH）を介してスイッチにアクセスします。
- （オプション）**[デバイス マネージャ（Device Manager）]** をクリックし、to view a graphical representation of Cisco MDS 9000 ファミリ スイッチ シャーシ、インストールされたモジュールを含む Cisco Nexus 5000 Series スイッチ シャーシ、Cisco Nexus 7000 Series スイッチ

シャーシ、あるいはCisco Nexus 9000 シリーズ スイッチ シャーシ、スーパーバイザ モジュール、各モジュール内の各ポートのステータス、電源、ファンアセンブリのグラフィック表を表示します。

- （オプション）**[HTTP]** をクリックして、そのスイッチのハイパーテキスト転送プロトコル（HTTP）を介してスイッチにアクセスします。
- （オプション）**[アカウンティング]** をクリックして、このスイッチに関連する [アカウンティング情報の表示] ウィンドウに移動します。
- （オプション）**[バックアップ]** をクリックして、[構成の表示] ウィンドウに移動します。
- （オプション）**[イベント（Events）]** をクリックしてイベント登録の表示, on page 362 ウィンドウに移動します。
- （オプション）**[Show Commands]** をクリックして、デバイスの show コマンドを表示します。Device Show Commands ページでは、コマンドを表示して実行できます。
- （オプション）**[実行中の構成を起動構成にコピー（Copy Running Config to Startup Config）]** をクリックして、実行構成をスタートアップ構成にコピーできます。
- [Generate tac-pac] をクリックして、Cisco DCNM のデバイスからテクニカル サポートを収集します。詳細については、「デバイスからのテクニカル サポートの収集」セクションを参照してください。

デバイスからテクニカル サポートの収集

Cisco DCNM Web クライアントのデバイスからテクニカル サポートを生成するときに、プロトコルを選択できます。Cisco DCNM Web UI でデバイスからテクニカル サポートを収集するには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。

Cisco DCNM によって検出されたすべてのスイッチのインベントリが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列のスイッチをクリックします。

そのスイッチに対応するスイッチのダッシュボードが表示されます。

ステップ 3 **[アクション（Actions）]** 領域で、**[tac-pac の生成（Generate tac-pac）]** をクリックします。

[tac-pac の生成（Generate tac-pac）] ダイアログ ボックスが表示されます。

ステップ 4 適切なオプション ボタンをクリックして、管理インターフェイスを選択します。

有効な値は、**default**、**vrf management**、および **vrf default** です。選択されたデフォルト値は、**default** です。

Note このオプションは、Nexus スイッチでのみ有効です。

ステップ 5 適切なオプション ボタンをクリックして、スイッチから DCNM へのトランスポート プロトコルを選択します。

有効な値は、**[TFTP]**、**[SCP]**、および **[SFTP]** です。

Note **[SCP]** または **[SFTP]** オプションを選択した場合は、DCNM サーバ クレデンシャルを入力します。

ステップ 6 [OK] をクリックします。

tac-pac が生成されてサーバに保存されると、ローカル マシンでファイルを開くか保存するためのダイアログ ボックスが表示されます。

デバイス マネージャ情報の表示

Note Windows 用 Cisco DCNM をインストールした後、ログオンするには、Cisco DCNM SAN サービスでクレデンシャルを編集して入力する必要があります。**[サービス（Services）] > [Cisco DCNM SAN サーバ（Cisco DCNM SAN Server）] > [Cisco DCNM SAN サーバ プロパティ（Cisco DCNM SAN Server Properties）] > [ログ オン（Log On）]** タブに移動します。このアカウント ラジオ ボタンを選択し、ユーザー名とパスワードを入力します。[OK] をクリックします。SSH にログオンし、DCNM サービスを停止します。DCNM サービスを開始したら、デバイス マネージャを使用できるようにする必要があります。

Note Linux 用 Cisco DCNM をインストールした後、デバイス マネージャが機能するために画面に表示される手順を実行します。デバイス マネージャには、Linux/OVA DCNM サーバで適切に設定されたグラフィカル環境が必要です。

スイッチのダッシュボードには、選択したスイッチの詳細が表示されます。

Procedure

ステップ 1 左のメニューバーで、**[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Swithces）]** の順に選択します。

Cisco DCNM Web クライアントによって検出されたスイッチのインベントリが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列のスイッチをクリックします。

そのスイッチに対応する **[スイッチ（Switch）]** ダッシュボードが、次の情報とともに表示されます。

ステップ 3 **[デバイス マネージャー（Device Manager）]** タブをクリックします。デバイス マネージャ ログイン ダイアログ ボックスが追加されます。デバイス マネージャ アプリケーションにログインします。デバイス マネージャはインストールしたスイッチ モジュール、スーパーバイザー モジュール、各モジュールの各ポートのステータス、電源モジュール、グラフィック表示のファン アセンブリの視覚的な表示を提供します。

デバイス マネージャの詳細については、次の URL にアクセスしてください。

[Cisco DCNM SAN クライアント オンライン ヘルプ（Cisco DCNM SAN Client Online Help）]

スイッチ ライセンスのインストール

Cisco DCNM Web UI からスイッチ ライセンスを再検出するには、以下の手順を実行します：

Procedure

ステップ 1 スイッチを選択します。 **[インベントリ（Inventory）]** > **[表示（View）]** > **[スイッチ（Switches）]**。

または、**[インベントリ（Inventory）]** > **[表示（View）]** > **[スイッチ（Switches）]** を選択できます。

ステップ 2 スイッチのダッシュボードで **[ライセンス（License）]** をクリックします。

ステップ 3 **[インストール（Install）]** をクリックして、スイッチ ライセンス ファイルをスイッチにインストールします。

[スイッチ ライセンス インストール（Switch License Install）] ウィンドウが表示されます。

ステップ 4 **[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 システムからライセンス ファイルを選択します。

ステップ 5 送信メソッドの選択。次のオプションを使用できます。

- TFTP
- SCP
- SFTP

ステップ 6 DCNM サーバに接続するためのユーザー名とパスワードを入力します。

ステップ 7 [インストール（Install）] をクリックします。

スイッチ ライセンスの再検出

Cisco DCNM Web UI からスイッチ ライセンスを再検出するには、以下の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**。

または、**[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Inventory）]** を選択できます。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択します。

ステップ 3 スイッチ ダッシュボードの **[ライセンス（License）]** タブをクリックします。

ステップ 4 **[再検出（Rediscover）]** をクリックして、スイッチのスイッチ ライセンスを再検出します。

スイッチ ライセンスの再検出には時間がかかります。

ステップ 5 **[最終更新（Last Updated）]** アイコンをクリックして、ライセンスを更新します。

インターフェイス

インターフェイスの show コマンドの表示

Cisco DCNM Web UI からインターフェイス show コマンドを表示するには、以下の手順実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。**[スイッチ（Switches）]** ウィンドウが選択した **[範囲（Scope）]** のすべてのスイッチのリストを表示しています。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 **[表示（Show）]** をクリックして、インターフェイス 表示コマンドを表示します。

[インターフェイスの show コマンド（Interface Show Commands）]ウィンドウは、コマンドを表示して実行するのに役立ちます。

インターフェイスの再検出

Cisco DCNM Web UI からインターフェイスを再検出するには、次の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。

[スイッチ（Switches）] ウィンドウが表示され、選択した**範囲**のすべてのスイッチのリストが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 **[再検出（Rediscover）]** をクリックして、選択されたインターフェイスを再検出します。たとえば、インターフェイスを編集または有効にした後、インターフェイスを再検出できます。

インターフェイス履歴の表示

Cisco DCNM Web UI からインターフェイス履歴を表示するには、次の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。

[スイッチ（Switches）] ウィンドウが選択した [範囲（Scope）] のすべてのスイッチのリストを表示しています。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4 **[インターフェイス履歴（Interface History）]** をクリックして、**[ポリシー名（Policy Name）]**、**[実行時間（Time of Execution）]** などのインターフェイス履歴の詳細を表示します。

VLAN

VLAN は、番号を割り当てることによって作成します。作成した VLAN は削除したり、アクティブ ステートから一時停止ステートに移行したりできます。

VLAN を構成するには、**[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列でスイッチをクリックします。

次の表で、このページに表示されるボタンを説明します。

表 3 : VLAN タブ

フィールド	説明
選択項目のクリア	選択したすべての VLAN の選択を解除できます。
追加	クラシカルイーサネットまたはファブリックパス VLAN を作成できます。

フィールド	説明
編集	VLAN を編集できます。
削除（Delete）	VLAN を削除できます。
シャットダウンなし	VLAN を有効にできます。
シャットダウン	VLAN を無効にすることができます。
表示	VLAN show コマンドを表示できます。

この項の内容は、次のとおりです。

VLAN の追加

Cisco DCNM Web UI から VLAN を追加するには、以下の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]**の順に選択します。

[スイッチ（Switches）] ウィンドウが選択した **[範囲（Scope）]** のすべてのスイッチのリストを表示しています。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 **[VLAN]** タブをクリックします。

ステップ 4 クラシカル イーサネットまたは Fabric Path VLAN を作成するために**[Add（追加）]**をクリックします。**[VLAN の追加（Add VLAN）]** ウィンドウで、次のフィールドを指定します。

a) **[Vlan ID（Vlan Id）]** フィールドにVLAN ID を入力します。

b) **[モード（Mode）]**フィールドで、クラシック イーサネットまたはファブリック パス VLAN を追加するかどうかを指定します。

c) **[管理状態オン（Admin State ON）]** チェックボックスを選択して、VLANをシャットダウンするかどうかを指定します。

VLAN の有効化

Cisco DCNM Web UI から VLAN を編集するには、以下の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** の順に選択します。

[スイッチ（Switches）] ウィンドウが選択した **[範囲（Scope）]** のスイッチの全リストともに表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 1 つ以上の VLAN を選択し、**[編集（Edit）]** をクリックします。

VLAN の削除

Cisco DCNM Web UI から VLAN を削除するために、次の手順を実行します。

手順

ステップ 1 **[インベントリ > 表示 > スイッチ（Inventory > View > Switches）]** の順に選択します。

[スイッチ（Switches）] ウィンドウが選択した **[スコープ（Scope）]** の全てのスイッチのリストを表示しています。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 **[VLAN]** タブをクリックします。

ステップ 4 削除する VLAN を選択し、**[削除（Delete）]** をクリックします。

VLAN のシャットダウン

Cisco DCNM Web UI から VLAN をシャットダウンするには、以下の手順を実行します。

手順

ステップ 1 **[インベントリ] > [表示] > [スイッチ]**の順に選択します。

[スイッチ（Switches）] ウィンドウが選択した **[範囲（Scope）]** のすべてのスイッチのリストを表示しています。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 **[VLAN]** タブをクリックします。

ステップ 4 **[シャットダウン（Shutdown）]**をクリックして、 VLAN を無効にします。

VLAN を有効にするには、**[シャットダウンしない（No Shutdown）]**ボタンをクリックします。たとえば、VLAN でトラフィック フローを開始する場合は、VLAN を有効にすることができます。

VLAN Show コマンドの表示

Cisco DCNM Web UI から VLAN show コマンドを表示するには、以下の手順実行します。

手順

ステップ 1 **[インベントリ > 表示 > スイッチ（Inventory > View > Switches）]** の順に選択します。

[スイッチ（Switches）] ウィンドウが表示され、選択した**範囲**のすべてのスイッチのリストが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列でスイッチを選択して、**[スイッチ ダッシュボード（Switch Dashboard）]** を表示します。

ステップ 3 **[VLAN]** タブをクリックします。

ステップ 4 **[表示（Show）]** をクリックして、VLAN 表示コマンドを表示します。VLAN の選択に基づいて、VLAN コマンドを表示できます。**[インターフェイスのコマンドの表示（Interface Show Commands）]** ウィンドウにコマンドが表示され、それらを実行できます。

FEX

ファブリック エクステンダ機能を使用すると、Cisco Nexus 2000 シリーズ ファブリック エクステンダと、それが接続されている Cisco NX-OS スイッチとの関連付けを管理できます。ファブリック エクステンダは、物理イーサネット インターフェイスまたはポート チャネルを介してスイッチに接続されます。ファブリック エクステンダは、デフォルトでは、シャーシ ID を割り当てるか、接続するインターフェイスに関連付けるまで、スイッチに接続できません。ファブリック エクステンダのホスト インターフェイス ポートをルーテッド ポートまたはレイヤ 3 ポートとして構成できます。ただし、このルーテッド インターフェイスにルーティング プロトコルを関連付けることはできません。

（注） FEX 機能は LAN デバイスでのみ使用できます。したがって、Cisco DCNM **[インベントリ スイッチ（Inventory Switches）]**に FEX が表示されます。 Cisco Nexus スイッチが SAN ファブリックの一部として検出された場合、FEX 機能は使用できません。FEX は、Cisco Nexus 1000V デバイスでもサポートされていません。

（注） FEX 接続の 4x10G ブレークアウトは、Cisco Nexus 9500 スイッチではサポートされていません。

（注） ファブリック エクステンダは、いくつか個別の物理イーサネット インターフェイスまたは最大 1 つのポート チャネル インターフェイスを通して、スイッチに接続可能です。

このセクションでは、Cisco DCNM を介して Cisco Nexus スイッチでファブリック エクステンダ（FEX）を管理する方法について説明します。

Cisco DCNM **[インベントリ（Inventory）] > [スイッチ（Switches）]** から FEX を作成および管理できます。

（注） FEX タブは、LAN デバイスを選択した場合にのみ表示されます。

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。

表 *4 : FEX*動作

フィールド	説明
追加（Add）	クリックして、新しい FEX を Cisco Nexus スイッチに追加します。
編集	アクティブな FEX オプション ボタンを選択し、[編集] をクリックして FEX 構成を編集します。 編集テンプレートを作成して、FEX の編集に使用できます。テンプレート タイプとして POLICY を選択し、サブ タイプとして FEX を選択します。
削除（Delete）	FEX オプション ボタンを選択し、[削除（Delete）] アイコンをクリックして、スイッチに関連付けられた FEX を削除します。
表示	選択した FEX ID のさまざまな構成の詳細を表示できます。ドロップダウンリストから以下を選択できます。 • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module それぞれの show コマンドの変数は、[変数（Variables）] 領域に表示されます。変数を確認し、**[実行（Execute）]** をクリックします。出力は **[出力（Output）]** 領域に表示されます。 FEX の表示テンプレートを作成できます。テンプレート タイプとして [SHOW] を選択し、サブ タイプとして [FEX] を選択します。

フィールド	説明
FEX 履歴	特定の FEX の FEX 構成タスクの履歴を表示できます。選択した FEX のイベント タイプ、ポリシー名、ステータス、実行時間、ユーザー名を確認できます。

表 *5: FEX* フィールドと説明

フィールド	説明
FEX ID	Cisco NX-OS デバイスに接続されているファブリック エクステンダを一意に識別します。
FEX の説明	ファブリック エクステンダ用に構成された説明。
FEX バージョン	スイッチに関連付けられている FEX のバージョンを指定します。
ピン接続	一度にアクティブである、ファブリック エクステンダの最大ピン接続アップリンク数を表す整数値です。
ステータス	Cisco Nexus スイッチに関連付けられた FEX のステータスを指定します。
モデル	FEX のモデルを指定します。
シリアル番号（Serial No.）	構成されたシリアル番号を指定します。 （注） この構成済みシリアル番号とファブリック エクステンダの実際のシリアル番号が同じでない場合、ファブリック エクステンダはアクティブになりません。
ポート チャネル	FEX がスイッチに物理的に接続されているポート チャネル番号を指定します。
イーサネット	FEX が接続されている物理インターフェイスを指します。
vPC ID	FEX 用に構成された vPC ID を指定します。

この章は、次の項で構成されています。

FEX を追加

Cisco DCNM Web UI から シングルホーム FEX を追加するには、次の手順を実行します。

始める前に

Cisco DCNM Web クライアントを介して、Fabric Extender（FEX、ファブリック エクステンダ）を Cisco Nexus スイッチに追加できます。FEX がスイッチに物理的に接続されている場合、FEX

は追加後にオンラインになります。FEXがスイッチに物理的に接続されていない場合、構成はスイッチに展開され、接続時に FEX が有効になります。

（注） **[Inventory（インベントリ）] > [Switches（スイッチ）] > [FEX] > [Add FEX（FEX を追加）]** を使用して、シングル ホーム FEX のみを作成できます。デュアルホーム FEX を作成するには、**[Configure（構成）] > [Deploy（展開する）] > [vPC]** から vPC ウィザードを使用します。

FEXを構成する前に、ローカルエリア ネットワーク（LAN）デバイスが正常に検出され、ローカル エリア ネットワーク（LAN）ログイン情報が設定されていることを確認してください。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [FEX]** を選択します。

[FEX] ウィンドウが表示されます。

ステップ 2 **[追加（Add）]** FEX アイコンをクリックします。

ステップ 3 [全般（General）] タブの **PORTCHANNEL** フィールドに、FEXに接続されているインターフェイス ポート チャネル番号を入力します。

ステップ 4 **[INT_RANGE]** フィールドに、FEX がスイッチに接続されているインターフェイス範囲を入力します。

（注） インターフェイスがすでにポートチャネルの一部である場合は、インターフェイス範囲に入らないでください。

ステップ 5 **[FEX_ID]** フィールドに、Cisco NX-OS デバイスに接続されている FEX の ID を入力します。

識別子は、100 から 199 までの整数値である必要があります。

ステップ 6 [追加] をクリックします。

構成されたシングルホーム FEX が、デバイスに関連付けられた FEX のリストに表示されます。

FEX の編集

Cisco DCNM Web UI から FEX を編集および展開するには、次の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [FEX]** を選択します。

[FEX] ウィンドウが表示されます。

ステップ 2 編集する必要がある FEX オプション ボタンを選択します。[FEX の**編集**（Edit FEX）] アイコンをクリックします。

ステップ 3 [構成の編集（Edit Configuration）] ウィンドウで、[ポリシー（Policy）] ドロップダウン リストから **[FEX の編集（Edit_FEX）]** を選択して、FEX 設定を編集します。

ステップ 4 必要に応じて、**[固定（pinning）]** フィールドと **[FEX_DESC]** フィールドを編集します。

（注） 最初に親スイッチのポート 33 を唯一のファブリック インターフェイスとして設定すると、48 のすべてのホスト インターフェイスがこのポートにピン接続されます。別のポート（たとえば 35）をプロビジョニングした場合、この手順を実行してホスト インターフェイスを再配布する必要があります。これにより、すべてのホスト インターフェイスがダウンし、ホスト インターフェイス 1 ～ 24 はファブリック インターフェイス 33 に、ホスト インターフェイス 25 ～ 48 はファブリック インターフェイス 35 にピン接続されます。

ステップ 5 [プレビュー（Preview）] をクリックします。

選択した FEX ID に対して生成された構成を表示できます。次に、FEX ID 101 の構成例を示します。

```
fex 101
pinning max-links 1
description test
```

ステップ 6 [プレビュー（Preview）] ウィンドウで構成の概要を確認した後、[構成の編集（Edit Configuration）] 画面で、**[展開（Deploy）]** をクリックしてスイッチの FEX を展開します。

VDC

このセクションでは、Cisco DCNM を介して Cisco Nexus 7000 スイッチで仮想デバイス コンテキスト (VDC) を管理する方法について説明します。

ネットワーク管理者（network-admin）ロールに指定されたユーザーは、仮想デバイスコンテキスト（VDC）を作成できます。VDC リソース テンプレートは、VDC が使用可能な物理デバイスの量を制限します。Cisco NX-OS ソフトウェアはデフォルトのリソース テンプレートを提供します。また、ユーザはリソース テンプレートを作成できます。

Cisco DCNMで **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** から VDC を作成および管理できます。Cisco DCNM は Cisco Nexus 7000 シリーズでのみ DCNM をサポートするため、アクティブな Cisco Nexus 7000 スイッチをクリックします。VDC の作成後は、インターフェイスの割り当て、VDC リソース制限、およびハイアベイラビリティ（HA）ポリシーを変更できます。

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。

表 *6 : VDC* オペレーション

フィールド	説明
追加（Add）	クリックして新しい vDC を追加します。

フィールド	説明
編集	アクティブな VDC ラジオ ボタンを選択し、[編集] をクリックして VDC 構成を編集します。
削除（Delete）	VDC を削除できます。アクティブな VDC ラジオ ボタンを選択し、[削除] をクリックして、デバイスに関連付けられた VDC を削除します。
再開	中断された VDC を再開できます。
Suspend	アクティブなデフォルト以外の VDC を停止できます。 VDC を停止する前に、VDC の実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。保存しなかった場合、実行コンフィギュレーションに対する変更が失われます。 （注） デフォルト VDC は停止できません。 **注意** VDC を停止すると、その VDC 上のすべてのトラフィックが中断されます。
再検出	デフォルト以外の VDC を停止状態から再開できます。VDC は、スタートアップ構成に保存された設定内容で再開します。
表示	選択した VDC に割り当てられているインターフェイスとリソースを表示できます。 [インターフェイス] タブでは、VDC に関連付けられている各インターフェイスのモード、管理ステータス、および動作ステータスを表示できます。 [リソース] タブでは、リソースの割り当てとこれらのリソースの現在の使用状況を表示できます。

表 *7: VRF* テーブルのフィールドと説明

フィールド	説明
名前	VDC の一意の名前を表示します。
タイプ	VDC のタイプを指定します。VDC には次の 2 つのタイプがあります。 • イーサネット • ストレージ

フィールド	説明
ステータス（Status）	VDC のステータスを指定します。
リソース制限モジュール タイプ	割り当てられたリソース制限とモジュール タイプを表示します。

フィールド	説明
HA-Policy • スーパーバイザ 1 台 • デュアル スーパーバイザ	

フィールド	説明
	回復不可能なVDC障害が発生した場合にCisco NX-OS ソフトウェアによって実行される処理を指定します。 HA ポリシーは、VDC の作成時に、シングル スーパーバイザ モジュールおよびデュアル スーパーバイザ モジュール構成に対して指定できます。HAポリシーのオプションは次のとおりです。 **シングル スーパーバイザ モジュール構成**： • 停止（Bringdown）：VDC を障害状態に移行します。障害状態から復旧するには、物理デバイスをリロードする必要があります。 • リロード（Reload）：スーパーバイザ モジュールをリロードします。 • 再起動（Restart）：VDC プロセスとインターフェイスをいったん削除し、スタートアップ コンフィギュレーションを使用して再起動します。 **デュアル スーパーバイザ モジュール構成**： • 停止（Bringdown）：VDC を障害状態に移行します。障害状態から復旧するには、物理デバイスをリロードする必要があります。 • 再起動（Restart）：VDC プロセスとインターフェイスをいったん削除し、スタートアップ コンフィギュレーションを使用して再起動します。 • スイッチオーバー（Switchover）：スーパーバイザ モジュールのスイッチオーバーを開始します。 作成した、デフォルト以外のVDCに対するデフォルトのHAポリシーは、シングルスーパーバイザ モジュール構成の場合は再起動、デュアル スーパーバイザ モジュール構成の場合はスイッチオーバーです。デフォルトVDCに対するデフォルトの HA ポリシーは、シングル スーパーバイザモジュール構成の場合はリロー

フィールド	説明
	ド、デュアル スーパーバイザ モジュール構成の場合はスイッチオーバーです。
Mac アドレス	デフォルト VDC には管理 MAC アドレスを指定します。
管理インターフェイス • IP Address Prefix • ステータス（Status）	VDC 管理インターフェイスの IP アドレスを指定します。ステータスは、インターフェイスがアップかダウンかを示します。
SSH	SSH ステータスを指定します。

（注） 初期構成後にネイバー デバイスの VDC ホスト名を変更しても、古い VDC ホスト名へのリンクは新しいホスト名に自動的に置き換えられません。回避策として、古い VDC ホスト名へのリンクを手動で削除することをお勧めします。

この章は、次の項で構成されています。

VDC の追加

Cisco DCNM Web UI から VDC を追加するには、次の手順を実行します。

始める前に

network-admin ロールを持つユーザ名を使用する物理デバイスが検出されたことを確認します。

VDC の帯域外管理を使用するには、管理インターフェイス（mgmt 0）用に IPv4 または IPv6 アドレスを取得します。

ストレージ VDC を作成して FCoE を実行します。ストレージ VDC をデフォルト VDC にすることはできません。デバイスには 1 つのストレージ VDC を保有できます。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** を選択します。

VDC ウィンドウが表示されます。

ステップ 2 **[追加（Add）]** アイコンをクリックします。

ステップ 3 ドロップダウン リストから、VDC タイプを選択します。

VDC は 2 つのモードで構成できます。

- イーサネット VDC の構成

- ストレージ VDC の構成

デフォルトの VDC タイプは Ethernet です。

ステップ 4 [OK] をクリックします。

イーサネット *VDC* の構成

Cisco DCNM Web UI からイーサネット モードの VDC を構成するには、次の手順を実行します。

手順

ステップ 1 一般パラメータ タブで VDCの **[名前（Name）]** 、 **[シングル スーパーバイザ HA ポリシー（Single supervisor HA-policy）]** 、 **[デュアル スーパーバイザ HA ポリシー（Dual supervisor HA-policy）]** と **[技術情報リミットモジュール タイプ（Resouce Limit - Module Type）]**を指定します。

ステップ 2 割り当てインターフェイス タブでVDC に割り当てられるネットワーク インターフェイス（専用インターフェイスのメンバーシップ）を選択します。

[次へ（Next）] をクリックします。

ステップ 3 リソースの割り当てタブで、VDC の技術情報制限を指定します。

ラジオ ボタンを選択し、**[既存のテンプレートからテンプレートを選択（Select a Template from existing Templates）]** または **[新しいリソース テンプレートを作成（Create a New Resource Template）]** を選択します。VDC リソース テンプレートは、VDC で使用可能な最小および最大リソースを指定します。VDC の作成時に VDC リソース テンプレートを指定しない場合は、Cisco NX-OS ソフトウェアはデフォルトのテンプレートであるvdc-defaultを使用します。

- 既存のテンプレートからテンプレートを選択を選択した場合、**[テンプレート名（Template Name）]** ドロップダウン リストから、**[なし（None）]**、**[global-default]**、または **[vdc-default]** を選択できます。

  テンプレート 技術情報の制限については、以下で詳しく説明します。

表 *8:* テンプレート 技術情報の制限

Resource	最小	最大
グローバル デフォルト VDC テンプレート技術情報の制限		
バンドルされたエニーキャスト		

Resource	最小	最大
IPv6 マルチキャスト ルート メモリ	8	8 ルート メモリの単位はメガバイトです。
IPv4 マルチキャスト ルート メモリ	48	48
IPv6 ユニキャスト ルート メモリ	32	32
IPv4 ユニキャスト ルート メモリ		
VDC デフォルト テンプレートのリソース制限		
モニタ セッション延長		
モニタ セッション mx の例外		
モニタ SRC INBANDの監視		
ポート チャネル		
モニタ DST ERSPAN の監視		
SPAN セッション		
VLAN		
バンドルされたエニーキャスト		
IPv6 マルチキャスト ルート メモリ		
IPv4 マルチキャスト ルート メモリ		
IPv6 ユニキャスト ルート メモリ		
IPv4 ユニキャスト ルート メモリ		
VRF		

- **[新しい技術情報 テンプレートを作成（Create New Resource Template）]** を選択した場合は、一意のテンプレート名を入力します。技術情報制限エリアで、技術情報の必要に応じて、最小制限と最大制限を入力します。

[Cisco DCNM Web クライアント（Cisco DCNM **Web Client**）] > **[インベントリ（Inventory）]** > **[スイッチ（Switches）]** > **[VDC]** を使用して、単一の VDC の個々のリソース制限を編集できます。

[次へ（Next）] をクリックします。

ステップ 4 認証タブでは、管理者にパスワードの設定を許可し、AAA サーバ グループを使用してユーザーを認証することもできます。

管理者ユーザーエリアで：

- 必要に応じて、**[パスワード強度チェックを有効にする（Enable Password Strength Check）]** チェックボックスをオンにします。
- **[Password（パスワード）]** フィールドに管理ユーザー パスワードを入力します。
- **[Confirm Password（パスワードを確認）]** フィールドに管理ユーザーパスワードを再度入力します。
- **[有効期限日（Expiry Date）]** フィールドで下矢印キーをクリックし、有効期限日ダイアログボックスで管理ユーザの有効期限を選択します。**[期限切れにしない（Never）]** ラジオボタンを選択して、パスワードを期限切れにしないようにすることもできます。

AAA サーバ グループ エリア内：

- **[グループ名（Group Name）]** フィールドに AAA サーバ グループ名を入力します。
- **[サーバ（Servers）]** フィールドに、ホスト サーバの IPv4 または IPv6 のアドレスまたは名前を 1 つまたは複数（カンマで区切る）入力します。
- **[タイプ（Type）]** フィールドで、ドロップダウン リストから サーバ グループのタイプを選択します。

[次へ（Next）] をクリックします。

ステップ 5 マネジメント Ip タブ内で IPv4 または IPv6 のアドレス情報を入力します。

[次へ（Next）] をクリックします。

ステップ 6 サマリ タブ内で VDC 構成を確認します。

パラメータを編集するには、**[前へ（Previous）]** をクリックします。

[展開する（Deploy）] をクリックして、デバイスに VDC を設定します。

ステップ 7 [展開する] タブに、VDC 展開のステータスが表示されます。

確認メッセージが表示されます。**[詳細情報（Know More）]** をクリックして、VDC を展開するために実行されるコマンドを表示します。

[完了（Finish）]をクリックしてVDC構成ウィザードを閉じ、デバイスに構成されているVDCのリストを表示するために戻ります。

ストレージ *VDC* の構成

Cisco DCNM Web UI からストレージ モードの VDC を構成するには、次の手順を実行します。

始める前に

デバイスで FCoE を実行する際には、個別のストレージ VDC を作成します。ストレージ VDC にできるのは、VDC のいずれか 1 つだけです。デフォルト VDC をストレージ VDC として設定することはできません。

イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送する共有インターフェイスを設定できます。この特定のケースでは、同じインターフェイスが複数の VDC に属します。共有インターフェイスはイーサネットVDCとストレージVDCの両方に割り当てられます。

手順

ステップ 1 一般パラメータ タブで VDCの **[名前（Name）]** 、 **[シングル スーパーバイザ HA ポリシー（Single supervisor HA-policy）]** 、 **[デュアル スーパーバイザ HA ポリシー（Dual supervisor HA-policy）]** と **[技術情報リミットモジュール タイプ（Resouce Limit - Module Type）]**を指定します。

ステップ 2 FCoE Vlan の割り当てタブで、ドロップダウン リストから使用可能な**[イーサネット Vdc（Ethernet Vdc）]** を選択します。

既存のイーサネット VLAN 範囲が表示されます。使用可能なイーサネット VDC を選択しない場合は、**[なし（None）]** を選択します。

ストレージ VDC には、指定のインターフェイスと指定の FCoE VLAN を割り当てます。

[次へ（Next）] をクリックします。

ステップ 3 インターフェイスの割り当てタブで、専用インターフェイスと共有インターフェイスを FCoE VDC に追加します。

（注） 専用インターフェイスはFCoEトラフィックだけを伝送し、共有インターフェイスはイーサネット トラフィックと FCoEトラフィックの両方を伝送します。

イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送する共有インターフェイスを設定できます。この特定のケースでは、同じインターフェイスが複数の VDC に属します。FCoE VLANおよび共有インターフェイスは、同じイーサネットVDCから割り当てることができます。

[次へ（Next）] をクリックします。

ステップ 4 認証タブでは、管理者にパスワードの設定を許可し、AAA サーバ グループを使用してユーザーを認証することもできます。

管理者ユーザーエリアで：

- 必要に応じて、**[パスワード強度チェックを有効にする（Enable Password Strength Check）]** チェックボックスをオンにします。
- **[Password（パスワード）]** フィールドに管理ユーザー パスワードを入力します。
- **[Confirm Password（パスワードを確認）]** フィールドに管理ユーザー パスワードを再度入力します。
- **[有効期限日（Expiry Date）]** フィールドで下矢印キーをクリックし、有効期限日ダイアログボックスで管理ユーザの有効期限を選択します。**[期限切れにしない（Never）]** ラジオボタンを選択して、パスワードを期限切れにしないようにすることもできます。

AAA サーバ グループ エリア内：

- **[グループ名（Group Name）]** フィールドに AAA サーバ グループ名を入力します。
- **[サーバ（Servers）]** フィールドに、ホスト サーバの IPv4 または IPv6 のアドレスまたは名前を 1 つまたは複数（カンマで区切る）入力します。
- **[タイプ（Type）]** フィールドで、ドロップダウン リストから サーバ グループのタイプを選択します。

[次へ（Next）] をクリックします。

ステップ 5 マネジメント Ip タブ内で IPv4 または IPv6 のアドレス情報を入力します。

[次へ（Next）] をクリックします。

ステップ 6 サマリ タブ内で VDC 構成を確認します。

パラメータを編集するには、**[前へ（Previous）]** をクリックします。

[展開する（Deploy）] をクリックして、デバイスに VDC を設定します。

ステップ 7 [展開する] タブに、VDC 展開のステータスが表示されます。

確認メッセージが表示されます。**[詳細情報（Know More）]** をクリックして、VDC を展開するために実行されるコマンドを表示します。

[完了（Finish）] をクリックして VDC 構成ウィザードを閉じ、デバイスに構成されている VDC のリストを表示するために戻ります。

VDC の編集

Cisco DCNM Web UI から VDC を編集するには、次の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** を選択します。

VDC ウィンドウが表示されます。

ステップ 2 編集する必要がある VDC ラジオ ボタンを選択します。VDC の **[編集（Edit）]** アイコンをクリックします。

ステップ 3 必要に応じてパラメータを変更します。

ステップ 4 概要タブで構成の概要を確認したら、新しい構成で VDC を**[展開（Deploy）]** をクリックします。

モジュールのインベントリ情報の表示

Cisco DCNM Web UI の 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 **[インベントリ（Inventory）] > [表示（View）] > [モジュール（Modules）]**の順に選択します。

[モジュール（Modules）] ウィンドウに、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。

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、モジュールのグループ名が表示されます。
- **[スイッチ（Switch）]** 列には、モジュールが検出される時にスイッチ名が表示されます。
- **[名前（Name）]** にはモジュール名が表示されます。
- **[ModelName]** にモデル名が表示されます。
- **[SerialNum]** 列には、シリアル番号が表示されます。
- **[2nd SerialNum（2 番目の SerialNum ）]** 列には、 2 番目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。
- **[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（Hardware 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。
- **[OperStatus]** 列には、デバイスの動作状態が表示されます。
- **[IO FPGA]** 列には、IO フィールド プログラマブル ゲート 配列（FPGA）バージョンが表示されます。
- **[MI FPGA]** 列には、MI フィールド プログラマブル ゲート 配列（FPGA）のバージョンが表示されます。

ライセンスのインベントリ情報の表示

Cisco DCNM Web UI のライセンス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 **[インベントリ] > [表示] > [ライセンス]** の順に選択します。

選択した範囲に基づいて **[ライセンス（Licenses）]** ウィンドウが表示されます。

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]**列には、スイッチのグループ名が表示されます。
- **[スイッチ（Switvh）]**列には、機能が有効になっているスイッチ名が表示されます。
- **[機能（Feature）]**には、インストールされている機能が表示されます。
- **[ステータス（Status）]**は、ライセンスの使用ステータスを表示します。
- **[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）]**列には警告メッセージが表示されます。

ディスカバリ

Cisco DCNM リリース 10.x 以降、Cisco DCNM Web Client では、**管理者**が**ユーザー**を 1 つ以上のデバイス範囲またはグループに関連付けることができます。つまり、ロールベースのアクセス制御（RBAC）に基づいて、関連するグループまたは範囲デバイスにのみアクセスして構成できます。他のユーザーの関連付けられたデバイスにアクセスできない場合でも、**[インベントリ（Inventory）] > [検出（Discovery）]** タブで検出されたすべてのデバイスを表示できます。

左側のメニュー バーから、**[管理（Administration）] > [管理ユーザー（Management Users）]** に移動します。ユーザーを作成してグループを関連付け、リモート認証を管理し、接続されているすべてのクライアントを表示できます。RBAC の詳細については、「ローカル ユーザーを管理」に移動してください。

LAN、LAN タスク、およびスイッチの追加、編集、再検出、パージ、および削除

Cisco DCNM Web クライアントは、Cisco DCNM-LAN デバイスによって取得された情報を報告します。

Tip 検出されたデバイスが現在のユーザーの範囲内にない場合、LAN テーブルの LAN デバイスのチェック ボックスは灰色表示されます。

この項の内容は、次のとおりです。

LAN スイッチの追加

Cisco DCNM Web UI から LAN スイッチを追加するために次の手順を実行します。

スイッチを DCNM に正常にインポートするには、ローカルまたはリモート AAA を介してスイッチで定義され、DCNM へのインポートに使用されるユーザーに次の権限が必要です。

- スイッチへの SSH アクセス
- SNMPv3 クエリを実行する権限
- **show** コマンドを実行する機能

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [LAN]** を選択します。

[スイッチ（Switch）] 列に LAN デバイスのリストが表示されます。

ステップ 2 **[追加（Add）]** アイコンをクリックして、LAN を追加します。

[LAN デバイスの追加（Add LAN Devices）] ダイアログ ボックスが表示されます。

ステップ 3 **[シード スイッチ（Hops from seed Switch）]** または **[スイッチ リスト（Switch List）]** からホップを選択します。フィールドは、選択内容によって異なります。

ステップ 4 このファブリックの**シード スイッチ** IP アドレスを入力します。

LAN スイッチ ディスカバリの場合、DCNM はシード スイッチに IPv4 アドレスと IPv6 アドレスの両方を許可します。

ステップ 5 オプションは選択した検出タイプによって異なります。たとえば、**[SNMPv3/SSH を使用する（Use SNMPv3/SSH）]** をオンにすると、さまざまなフィールドが表示されます。

ステップ 6 ドロップダウン リストをクリックし、**Auth-Privacy** セキュリティ レベルを選択します。

ステップ 7 **[コミュニティ（Community）]** またはユーザーの資格情報を入力します。

ステップ 8 現在のユーザーの範囲内にある LAN グループの候補から LAN グループを選択します。

Note DCNM サーバを選択し、**[追加（Add）]** をクリックして LAN スイッチを追加します。

ステップ 9 **[次へ（Next）]** をクリックして、シャロー検出を開始します。

ステップ 10 **[LAN 検出（LAN Discovery）]** ウィンドウでは、スイッチ名の列の横にあるチェックボックスを使用してすべてのスイッチを選択するか、個々のスイッチを選択できます。[前へ]をクリックして、戻ってパラメータを編集します。

Note .

- [状態（Status）] 列で、スイッチの状態が**タイムアウト**または**接続不可**の場合、これらのスイッチは追加できません。到達可能でまだ管理されていないスイッチのみを選択できます。使用できないスイッチのチェックボックスは無効になっています
- DCNM で LAN デバイスを追加または検出すると、検出プロセスの一部として java が使用されます。ファイアウォールがプロセスをブロックすると、TCP 接続ポート 7 が検出プロセスとして使用されます。**cdp.discoverPingDisable** サーバ プロパティが **true** に設定されていることを確認します。**[Web UI]、[Administration]、[DCNM Server]、[Server Properties]** の順に選択して、サーバ プロパティを設定します。

ステップ 11 スイッチを選択して **[追加（Add）]** をクリックし、スイッチをスイッチ グループに追加します。

1 つ以上のシード スイッチに到達できない場合、シャロー [検出（Discovery）] ウィンドウに「不明」と表示されます。

ローカル エリア ネットワーク（LAN）デバイスの編集

Cisco DCNM Web UI から ローカル エリア ネットワーク（LAN）デバイスを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [ローカル エリア ネットワーク（LAN）スイッチ（LAN Switches）]** を選択します。

ステップ 2 編集するローカル エリア ネットワーク（LAN）の隣にあるチェックボックスを選択し、**[編集（Edit）]** アイコンをクリックします。

[ローカル エリア ネットワーク（LAN）の編集（Edit LAN）] ダイアログボックスが表示されます。

ステップ 3 [Username] と [Password] を入力します。

Note 資格情報または管理状態を変更するには、**[資格情報（Credential）]** または **[管理状態（Management State）]** を選択します。**[資格情報（Credential）]**が選択されている場合、SNMP バージョンと認証プライバシー v3、ユーザー名、またはパスワードを変更できます。**[管理状態（Management State）]** が選択されている場合、ステータスを管理対象または非管理対象に変更できます。

ステップ 4 ローカル エリア ネットワーク（LAN）ステータスを **[管理対象（Managed）]** または **[管理対象外（Unmanaged）]** として選択します。

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

ローカルエリアネットワーク（LAN）デバイス を Cisco DCNM から削除

Cisco DCNM から ローカルエリアネットワーク（LAN）スイッチを削除できます。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [LAN スイッチ（LAN Switches）]** を選択します。

ステップ 2 削除するローカルエリアネットワーク（LAN）の横にあるチェック ボックスをオンにし、**[削除（Delete）]** をクリックして、スイッチとそのすべてのデータを削除します。

ステップ 3 **[はい（Yes）]**をクリックして、ローカルエリアネットワーク（LAN）デバイスを確認します。

タスクの下での LAN デバイスの移動

Cisco DCNM Web クライアントを使用して、タスクの LAN デバイスを別のサーバーに移動できます。この機能はフェデレーション セットアップでのみ使用でき、[LAN の移動（Move LAN）] がフェデレーション セットアップ画面に表示されます。

ダウンしているサーバーからアクティブなサーバーーに ローカルエリア ネットワーク（LAN）を移動できます。管理状態はそのままです。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [LAN スイッチ]** を選択します。

ステップ 2 LAN テーブルから LAN デバイスを選択します。[移動（Move）] をクリックします。

ステップ 3 **[LAN タスクを別の DCNM サーバーに移動（Move LAN Tasks to another DCNM Server）]** ダイアログ ボックスで、移動する LAN デバイスを入力し、DCNM サーバーを指定します。

選択したタスク配下のすべての LAN デバイスが移動されます。

LAN タスクの再検出

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [LAN スイッチ（LAN Switches）]** を選択します。

ステップ 2 **[LAN を再検出（Rediscover LAN）]**をクリックします。

ステップ 3 ポップアップ ウィンドウで **[はい（Yes）]** をクリックして、LAN を再検出します。

管理されているファブリックの追加、編集、再検出、消去と削除。

Cisco DCNM クライアントは、Cisco DCNM-SAN に通知されているファブリックについて、Cisco DCNM-SAN によって取得された情報をレポートします。SAN スイッチを表示するには、**[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（ISAN Switches）]** を選択します。

SAN スイッチ ページのステータス列には、ファブリックのステータスを表示します。

- Manage Continuously：Cisco DCNM-SAN サーバーが起動すると、ファブリックは自動的に管理対象となり、このオプションが管理対象外に変更されるまで継続して管理されます。
- Manage：ファブリックは、それを表示する DCNM-SAN のインスタンスがなくなるまで、Cisco DCNM-SAN サーバによって管理されます。
- Unmanage：Cisco DCNM-SAN サーバはファブリックの管理を停止します。

この項の内容は、次のとおりです。

ファブリックの追加

Before you begin

新しいファブリックを検出する前に、スイッチに SNMP ユーザーを作成していることを確認してください。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

[SAN スイッチ（SAN Switches）] ウィンドウに、Cisco DCNM-SAN によって管理されているファブリックがあれば、そのリストが表示されます。

ステップ 2 **[追加（Add）]** をクリックして、新しいファブリックを追加します。

[ファブリックの追加（Add Fabric）] ウィンドウが表示されます。

ステップ 3 このファブリックの**ファブリック シード スイッチ** IP アドレスを入力します。

ステップ 4 (Optional) **SNMP** チェックボックスをオンにして、SNMPv3 または SSH を使用します。[SNMP] チェックボックスをオンにすると、**[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 5 このファブリックに対して**ユーザー名**と**パスワード**を入力します。

ステップ 6 **[Auth-Privacy]** ドロップダウン リストからプライバシー設定を選択します。

ステップ 7 (Optional) **[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て、新しいファブリックを検出するために提供された VSAN に含まれる VSAN リストまたは除外される VSAN リストを指定します。

ステップ 8 (Optional) **[すべてのファブリックで NPV 検出を有効にする（Enable NPV Discovery in all Fabrics）]** チェックボックスをオンにします。[すべてのファブリックで NPV 検出を有効にする（Enable NPV Discovery in all Fabrics）] をオンにすると、以前に検出されたすべてのファブリックに変更が適用されます。

ステップ 9 **[オプション（Options）]** をクリックし、**UCS ユーザー名**と **UCS パスワード**を指定します。

ステップ 10 **[DCNM サーバ（DCNM Server）]** ドロップダウン リストから DCNM サーバを選択します。

Note このオプションは、フェデレーションのセットアップだけに適用できます。

ステップ 11 **[追加（Add）]** をクリックすると、このファブリックの管理が開始されます。

Cisco DCNM Web クライアントから単一または複数のファブリックを削除できます。

ファブリックを削除しています

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

ステップ 2 削除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 **[削除（Delete）]** をクリックして、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。

ファブリックの編集

Cisco DCNM Web UI からファブリックを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

ステップ 2 編集するファブリックの隣にあるチェックボックスを選択し、**[編集（Edit）]**アイコンをクリックします。

[ファブリックの編集（Edit Fabric）] ダイアログボックスが表示されます。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 3 新しいファブリックの **[名前（Name）]** を入力します。

ステップ 4 (Optional) [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 5 **[ユーザー名（Username）]** および **[パスワード（Password）]** 、[プライバシー（privacy）] 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、DCNM 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 6 ファブリック管理状態を **[管理対象、非管理対象（Managed, Unmanaged）]** または **[継続的に管理（Managed Continuously）]** に変更します。

ステップ 7 [Apply] をクリックして、変更内容を保存します。

ステップ 8 パスワードを変更するには、Cisco DCNM Web UI から移動し次の手順を実行します。

a) **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

b) ファブリック スイッチのパスワードを変更するファブリックを選択します。

c) **[編集（Edit）]** をクリックし、ファブリックの管理を解除し、新しいパスワードを指定してから、ファブリックを管理します。

新しいパスワードがデータベースで検証されないため、ファブリックを開くことができません。

[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 資格情報（SAN Credentials）] に移動して、パスワードを検証できます。

ファブリックを別のサーバ フェデレーションに移動する

この機能はフェデレーション セットアップでのみ使用でき、Move Fabric はフェデレーション セットアップ画面にのみ表示されます。

ダウンしているサーバーからアクティブサーバにファブリックを移動できます。管理状態はそのままです。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

ステップ 2 別のサーバに移動するファブリックを選択し、**[移動（Move）]**をクリックします。

ステップ 3 **[ファブリックの移動]** ダイアログ ボックスで、ファブリックを移動する DCNM サーバを選択します。

[To DCNM Server] ドロップダウン リストには、アクティブなサーバだけが表示されます。

Note ファブリックのステータスは、数分間 **[管理対象外（Unmanaged）]** と表示され、その後 **managedContinuously** と表示されます。

ファブリックの再検出

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

ステップ 2 ファブリックの横にあるチェック ボックスをオンにして、**[再検出]** をクリックします。

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。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

ステップ 2 ファブリックの横にあるチェック ボックスをオンにして、**[再検出（Purge）]**ファブリック アイコンをクリックします。

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。

ファブリックは消去されます。

UCS ファブリック インターコネクト統合

リリース 11.3(1) から、UCS FI デバイスを検出して管理できます。

ディスカバリを有効にする

Cisco DCNM が UCS FI サーバ ブレードおよびサービス プロファイル情報を検出できるようにするには、**server.properties** ファイルを変更する必要があります。

[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)] をCisco DCNM Web UIから選択します。**fabric.enableUcsHttpDiscovery** プロパティを見つけます。この値が **[true]** に設定されていることを確認してください。

UCS FI デバイスの検出

リリース 11.3(1) 以降、Cisco DCNM は Web UI から UCS FI サーバー ブレードとサービス プロファイルを検出できます。

Cisco DCNM Web UI から LAN デバイスを編集するには、以下の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）]** を選択します。

[SAN Switches] ウィンドウには、Cisco DCNM-SAN によって管理されているファブリックがあれば、そのリストが表示されます。

ステップ 2 **[追加（Add）]**（+）アイコンをクリックして、新しいファブリックを追加します。

[ファブリックの追加（Add Fabric）] ウィンドウが表示されます。

ステップ 3 このファブリックの**ファブリック シード スイッチ** IP アドレスを入力します。

ステップ 4 （任意） **SNMP** チェックボックスをオンにして、SNMPv3 または SSH を使用します。

[SNMP] チェックボックスをオンにすると、[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 5 ファブリックに対してユーザー名とパスワードを入力します。

ステップ 6 **[Auth-Privacy]** ドロップダウン リストからプライバシー設定を選択します。

ステップ 7 （任意） **[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て、新しいファブリックを検出するために提供された VSAN に含まれる VSAN リストまたは除外される VSAN リストを指定します。

ステップ 8 （任意） **[すべてのファブリックで NPV 検出を有効にする（Enable NPV Discovery in all Fabrics）]** チェックボックスをオンにします。

[すべてのファブリックで NPV 検出を有効にする（Enable NPV Discovery in all Fabrics）] をオンにすると、以前に検出されたすべてのファブリックに変更が適用されます。

（注） デフォルトでは、Cisco UCS FI はNPV モードです。したがって、**[すべてのファブリックで NPV 検出を有効にする（Enable NPV Discovery in All Fabrics）]** チェックボックスをオンにすることをお勧めします。

ステップ 9 **[オプション]** をクリックし、UCS ユーザー名と UCS パスワードを指定します。

（注） ユーザー名とパスワードは SNMP ログイン情報です。一方、UCS ユーザー名とパスワードは UCS FI CLI 管理者ログイン情報です。

ステップ 10 DCNM サーバー ドロップダウン リストから DCNM サーバーを選択します。

このオプションは、フェデレーションのセットアップだけに適用できます。

ステップ 11 **[追加（Add）]** をクリックすると、このファブリックの管理が開始されます。

Cisco DCNM Web クライアントから単一または複数のファブリックを削除できます。

（注） UCS FI は、SNMP ユーザー管理の使用を禁止しています。

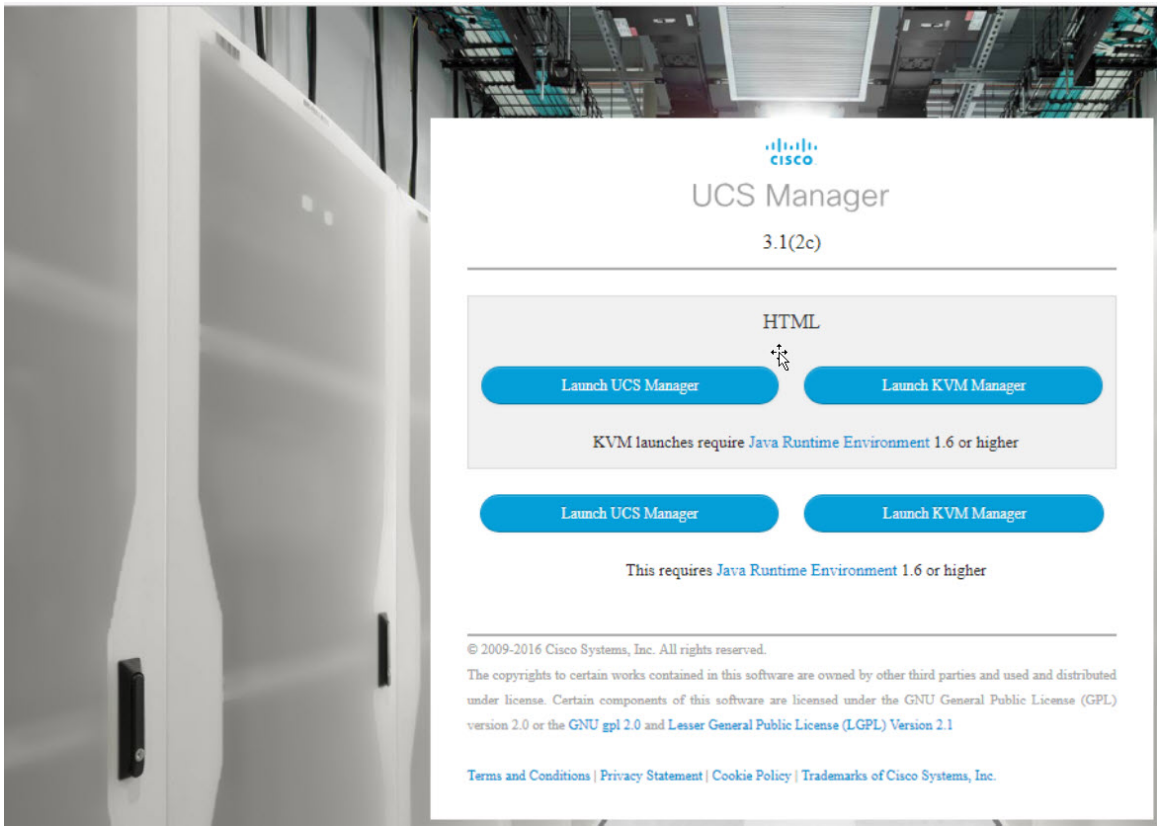
UCS FI での SNMP ユーザーの作成

UCS FI で別の SNMP ユーザーを作成するには、次の手順に従います。

手順

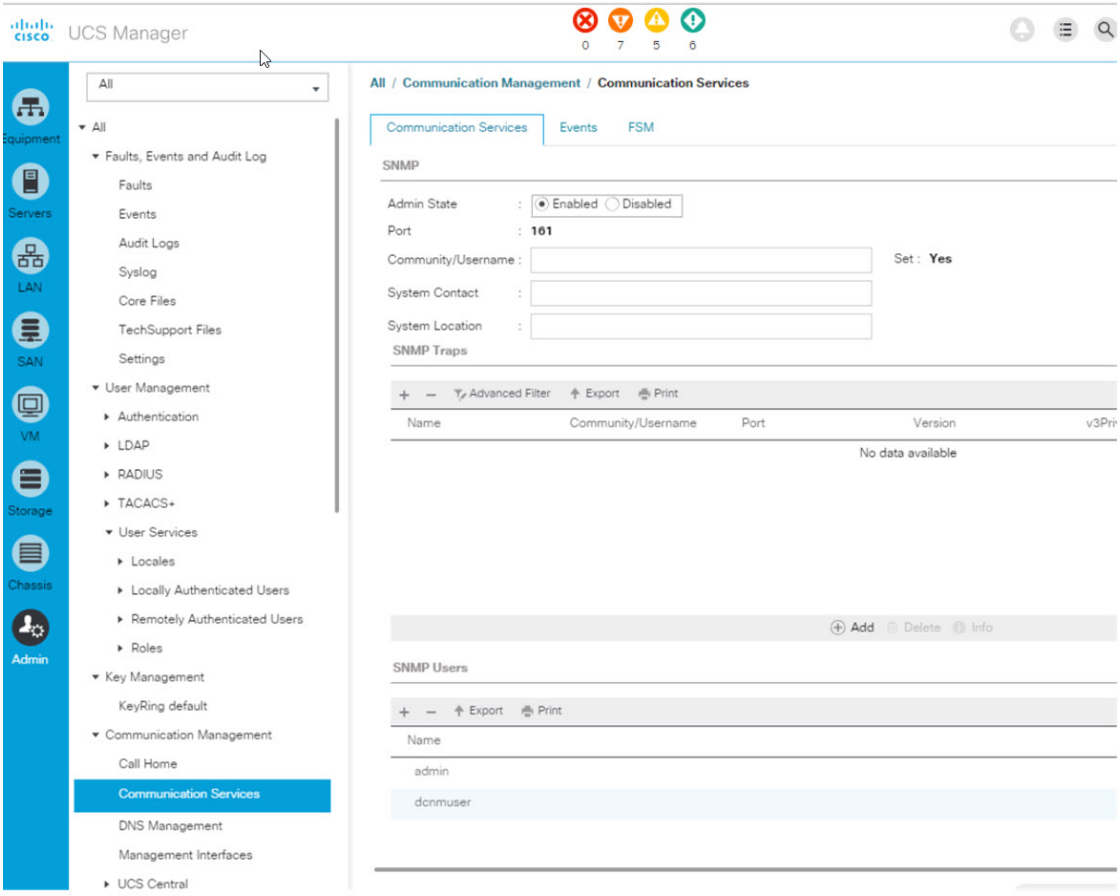
ステップ 1 UCS Manager にログインします。

Web ブラウザに適切な UCS FI IP アドレスを入力し、**[UCS Manager の起動（Launch UCS Manager（]** をクリックします。



ステップ 2 **[Admin（管理者）]** -> **[Communication Management（通信管理）]** -> **[Communication Services（通信サービス）]** をクリックします。

ステップ 3 SNMP セクションの **[管理状態Admin State]** フィールドで、**[有効化（Enabled）]** を選択します。



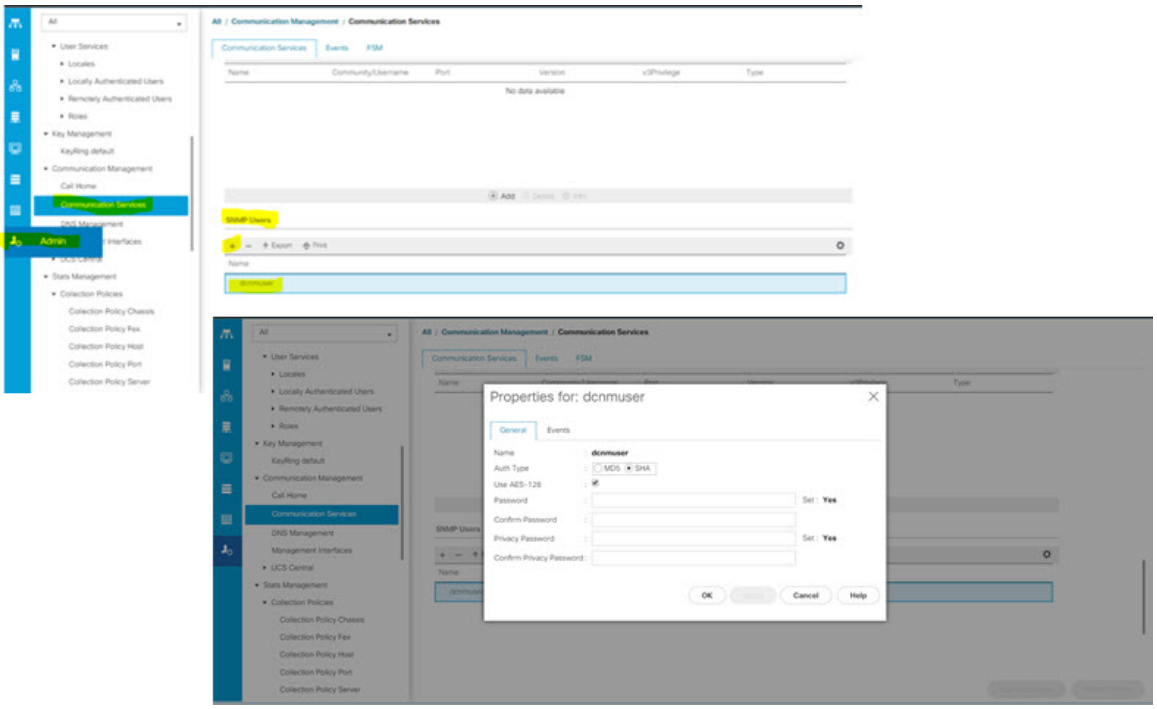
ステップ 4 新しい SNMP ユーザーを作成し、ログイン情報を提供します。

UCS Manager リリース 3.2(3) およびそれ以降のリリースでは、SNMPv3 が連邦情報処理標準（FIPS） モードの場合、MD5 認証をサポートしていません。

または、AES-128 暗号化で SHA を使用します。

UCS FI は、SHA_AES 認証タイプのみ (MD5 ではない) を介した SNMP 通信をサポートします。したがって、DCNM が **dcnmuser** などの共通ユーザーを使用してスイッチと FI の両方と通信できるように、UCS FI とファブリック内のすべてのスイッチの両方で SNMP ユーザーを設定する必要があります。

ステップ 5 UCS FI で **dcnmuser** を設定し、SNMP パスワードを **password1** として設定します。これは、UCS FI の**管理者または読み取り専用 CLI ユーザー** パスワード (**password2** など) とは異なる場合があることに注意してください。



ファブリック内のすべてのスイッチで、認証タイプが SHA_AES の **network-admin** または **network-operator** として同じ SNMP ユーザー **dcnmuser** を構成する必要があります。

```
MDS9396T-174145# show run | i dcnmuser
username dcnmuser password **** role network-admin
snmp-server user dcnmuser network-admin auth sha **** priv aes-128
**** localizedkey
MDS9396T-174145#

MDS9396T-174145# show snmp user
_____________________________________________________________________
                    SNMP USERS
_____________________________________________________________________
User            Auth  Priv(enforce) Groups               acl_filter
____            ____  ____________  ______               __________
admin           md5   des(no)       network-admin
dcnmuser        sha   aes-128(no)   network-admin
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________


User            Auth  Priv
____            ____  ____
```

これは、Cisco NPV スイッチにも当てはまります。

```
MDS9132T-1747# show feature | i npv
npv                   1         enabled

MDS9132T-1747# show snmp user
_____________________________________________________________________
                    SNMP USERS
_____________________________________________________________________
User            Auth  Priv(enforce) Groups               acl_filter
____            ____  ____________  ______               __________
```

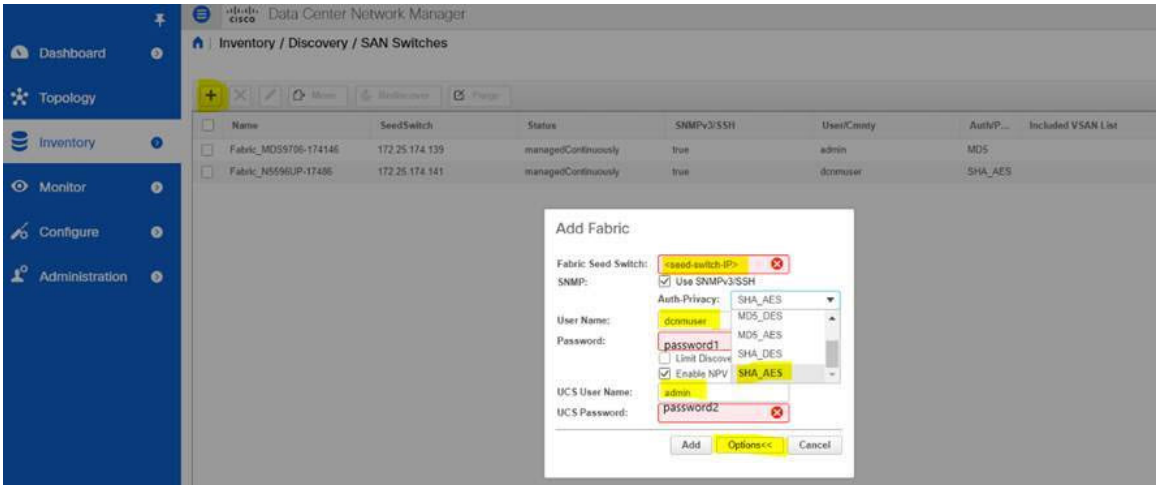
```
admin           md5   des(no)       network-admin
dcnmuser        sha   aes-128(no)   network-admin       network-operator
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________

User            Auth  Priv
____            ____  ____
```

ステップ 6 USC FI とスイッチが同じ資格情報、username: **dcnmuser** および password: **password1** を使用してアクセス可能になった後、ファブリックを検出できます。

[インベントリ（Inventory）] > [検出（Discovery）] > [SAN スイッチ（SAN Switches）] を選択して、ファブリックを検出します。

UCS FI の場合、username: **admin または読み取り専用 CLI ユーザー名**と password: **password2** を使用する必要があることに注意してください。



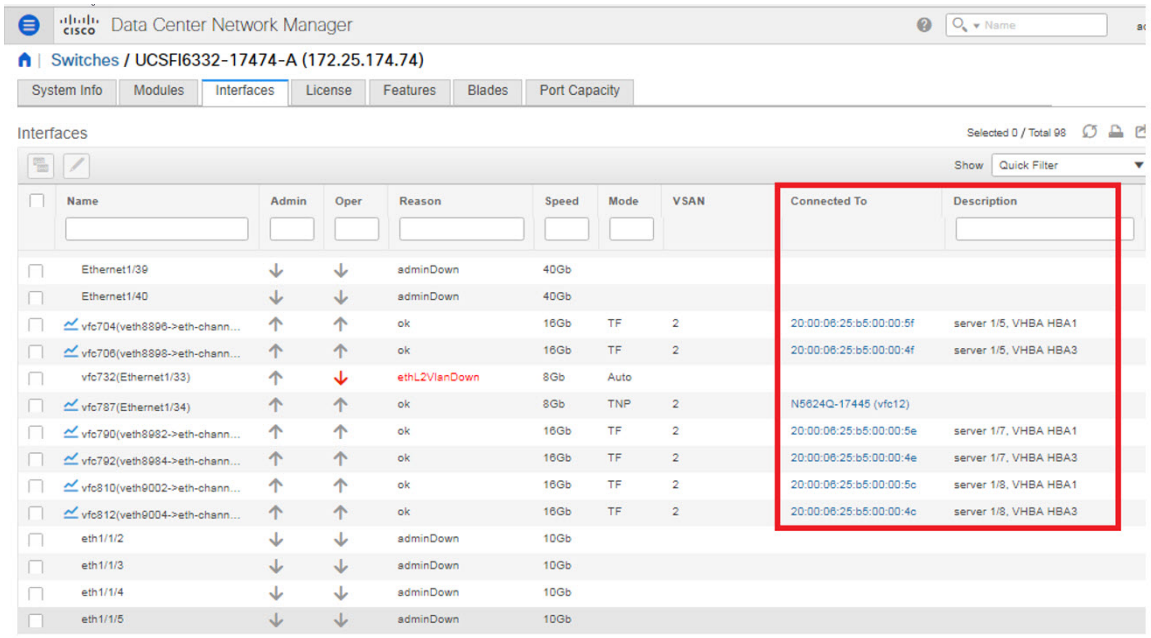
ステップ 7 UCF FI スイッチが Cisco DCNM **[Web UI] > [インベントリ（Inventory）] > [スイッチ（Switches）]** にリストされていることを確認します。

これらのスイッチのステータスが正しいことを確認してください。

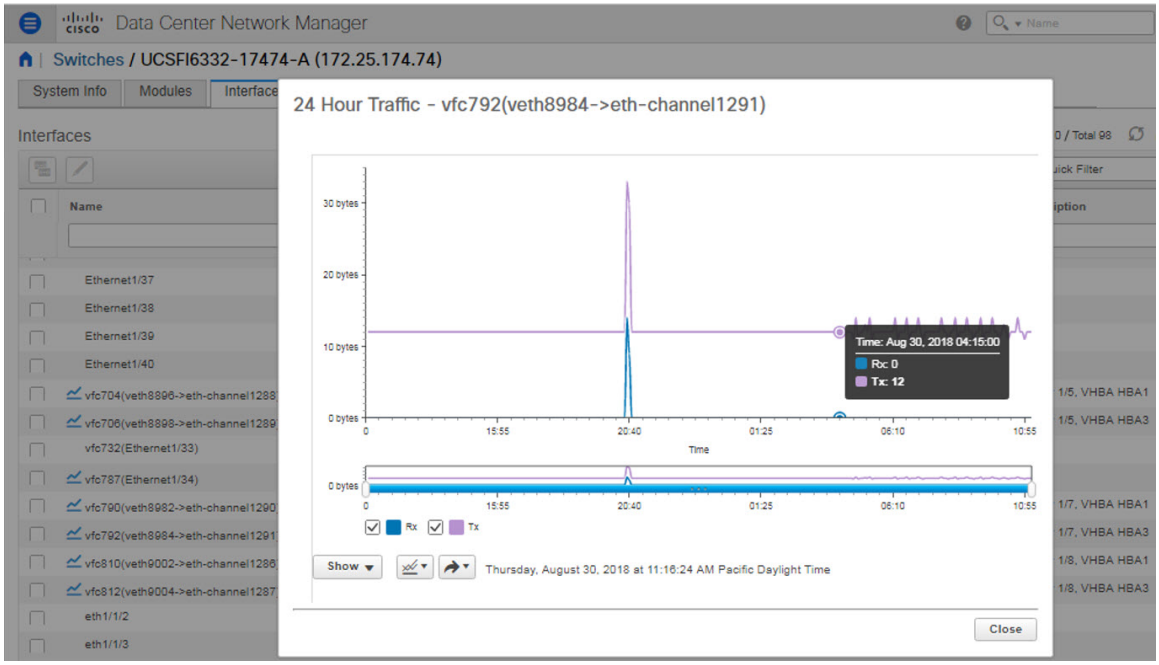
インベントリでの UCS FI スイッチの表示

Cisco DCNM Web クライアントで、**[Inventory（インベントリ）] > [Switches（スイッチ）] > [UCSFI] > [Interfaces（インターフェイス）]** から UCSFI スイッチのインターフェイスを表示できます。

インターフェイス タブには、UCS FI インターフェイスと、それらが接続するサーバー ブレードが表示されます。

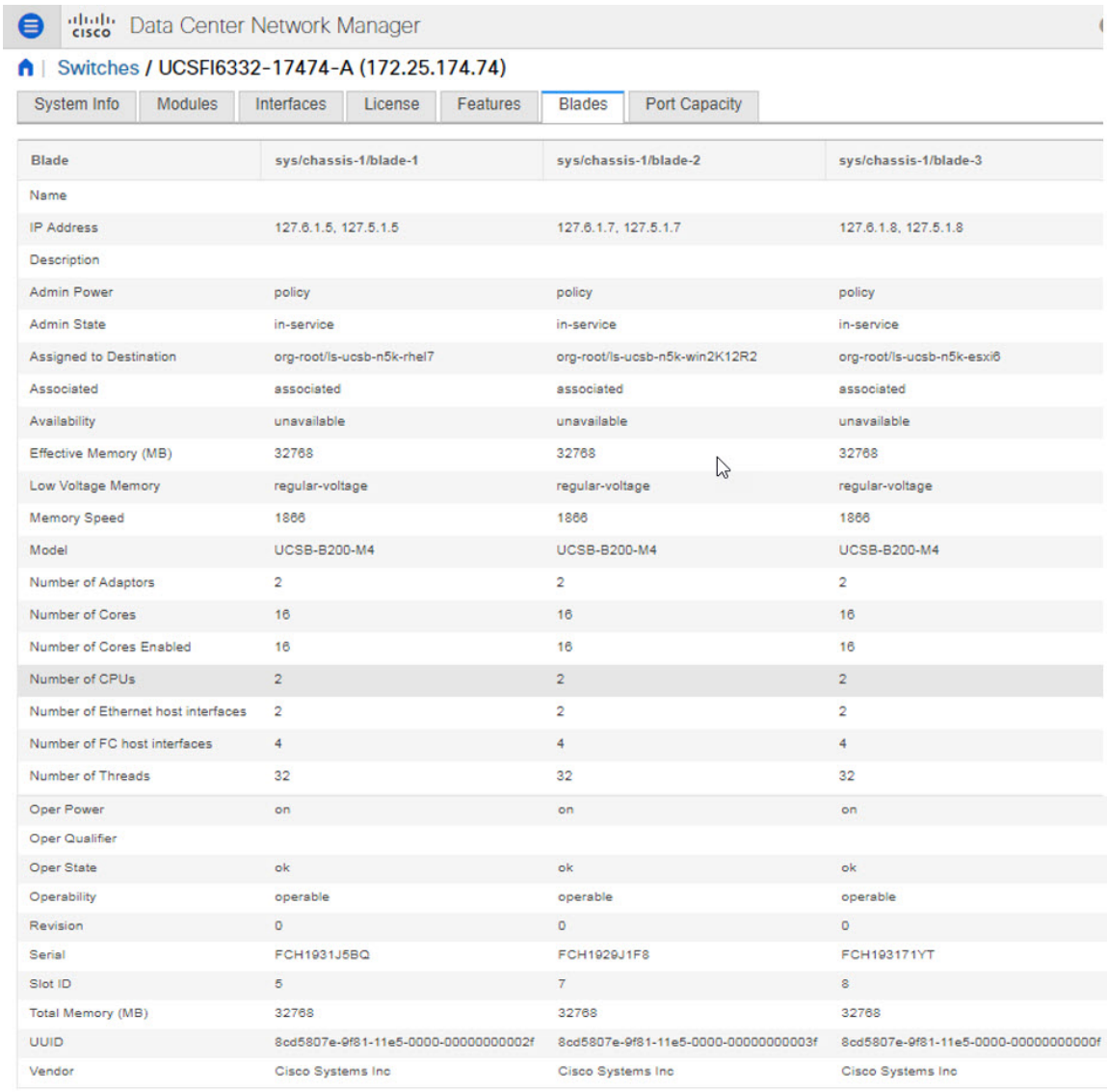


名前列の下のグラフ アイコンをクリックして、そのポートの 24 時間のトラフィック データを表示します。



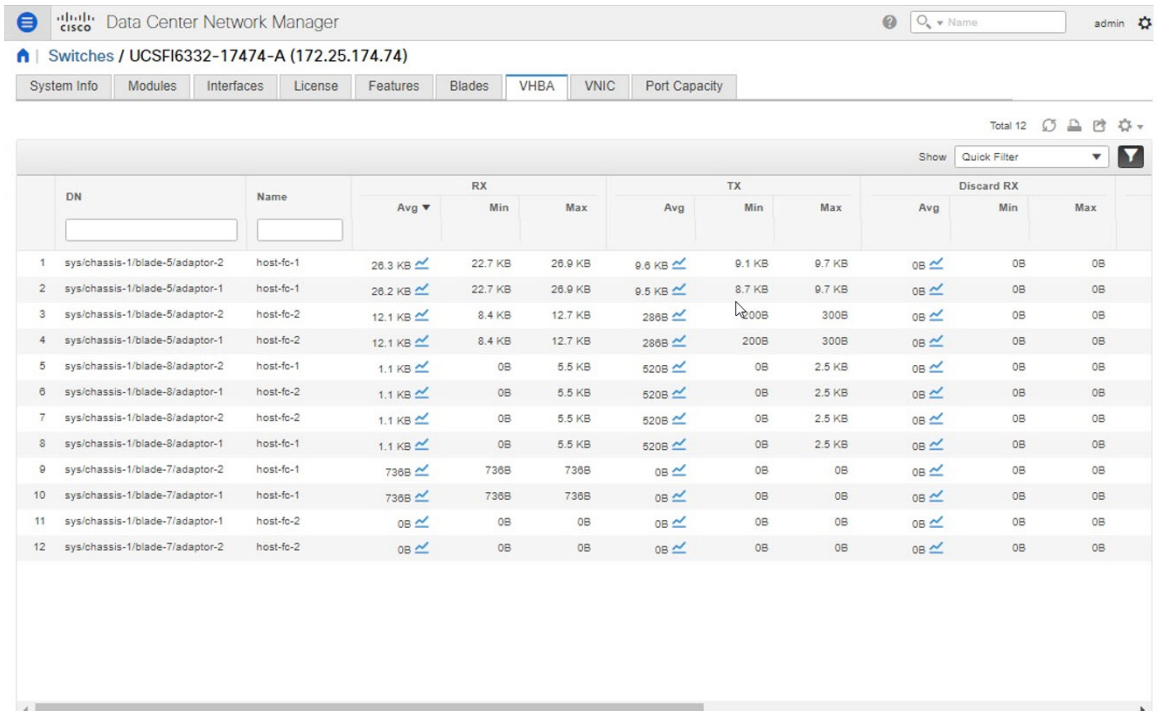
システム情報タブには、セカンダリ UCS FI に対応するプライマリ UCS FI IP が表示されます。

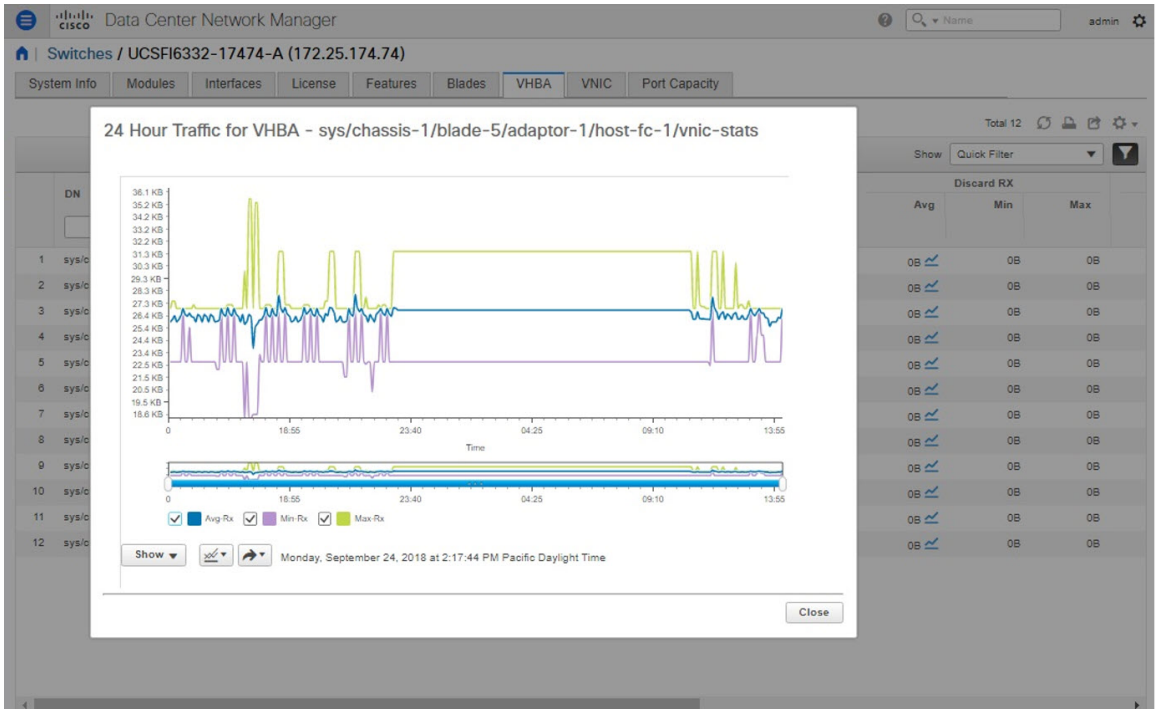
[ブレード（Blades）] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。冗長セットアップのプライマリ UCS FI またはスタンドアロン UCS FI のみが表示されます。



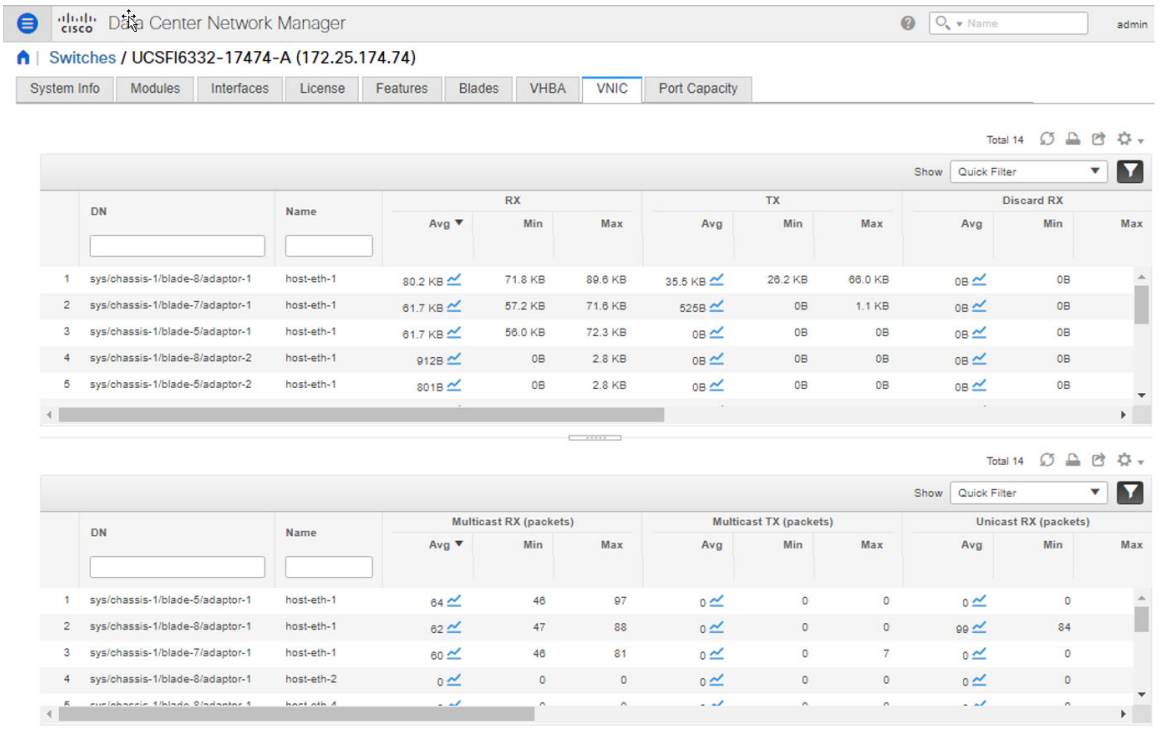
Blade	sys/chassis-1/blade-1	sys/chassis-1/blade-2	sys/chassis-1/blade-3
Name			
IP Address	127.6.1.5, 127.5.1.5	127.6.1.7, 127.5.1.7	127.6.1.8, 127.5.1.8
Description			
Admin Power	policy	policy	policy
Admin State	in-service	in-service	in-service
Assigned to Destination	org-root/ls-ucsb-n5k-rhel7	org-root/ls-ucsb-n5k-win2K12R2	org-root/ls-ucsb-n5k-esxi6
Associated	associated	associated	associated
Availability	unavailable	unavailable	unavailable
Effective Memory (MB)	32768	32768	32768
Low Voltage Memory	regular-voltage	regular-voltage	regular-voltage
Memory Speed	1866	1866	1866
Model	UCSB-B200-M4	UCSB-B200-M4	UCSB-B200-M4
Number of Adaptors	2	2	2
Number of Cores	16	16	16
Number of Cores Enabled	16	16	16
Number of CPUs	2	2	2
Number of Ethernet host interfaces	2	2	2
Number of FC host interfaces	4	4	4
Number of Threads	32	32	32
Oper Power	on	on	on
Oper Qualifier			
Oper State	ok	ok	ok
Operability	operable	operable	operable
Revision	0	0	0
Serial	FCH1931J5BQ	FCH1929J1F8	FCH193171YT
Slot ID	5	7	8
Total Memory (MB)	32768	32768	32768
UUID	8cd5807e-9f81-11e5-0000-00000000002f	8cd5807e-9f81-11e5-0000-00000000003f	8cd5807e-9f81-11e5-0000-00000000000f
Vendor	Cisco Systems Inc	Cisco Systems Inc	Cisco Systems Inc

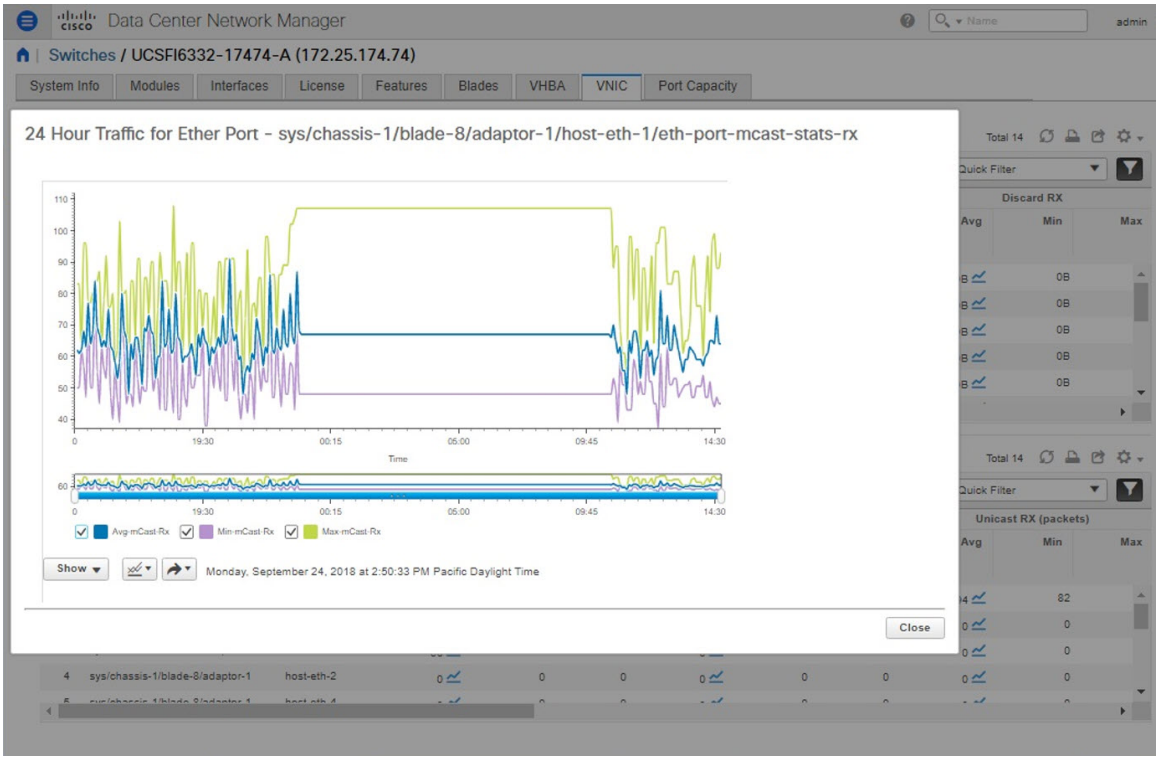
[vHBA] タブには、その特定の UCS FI の vHBA のリストが表示されます。グラフアイコンをクリックして、vHBA の 24 時間のトラフィックを表示します。





[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。


Data Center Network Manager
admin
Switches / UCSFI6332-17474-A (172.25.174.74)
System Info
Modules
Interfaces
License
Features
Blades
VHBA
VNIC
Port Capacity
Total 14
Show
Quick Filter
DN
Name
RX
TX
Discard RX
Avg
Min
Max
1 sys/chassis-1/blade-8/adaptor-1 host-eth-1 80.2 KB 71.8 KB 89.6 KB 35.5 KB 26.2 KB 66.0 KB 0B 0B
2 sys/chassis-1/blade-7/adaptor-1 host-eth-1 61.7 KB 57.2 KB 71.6 KB 525B 0B 1.1 KB 0B 0B
3 sys/chassis-1/blade-5/adaptor-1 host-eth-1 61.7 KB 56.0 KB 72.3 KB 0B 0B 0B 0B 0B
4 sys/chassis-1/blade-8/adaptor-2 host-eth-1 912B 0B 2.8 KB 0B 0B 0B 0B 0B
5 sys/chassis-1/blade-5/adaptor-2 host-eth-1 801B 0B 2.8 KB 0B 0B 0B 0B 0B
Multicast RX (packets)
Multicast TX (packets)
Unicast RX (packets)
1 sys/chassis-1/blade-5/adaptor-1 host-eth-1 64 46 97 0 0 0 0 0
2 sys/chassis-1/blade-8/adaptor-1 host-eth-1 62 47 88 0 0 0 99 84
3 sys/chassis-1/blade-7/adaptor-1 host-eth-1 60 46 81 0 0 7 0 0
4 sys/chassis-1/blade-8/adaptor-1 host-eth-2 0 0 0 0 0 0 0 0

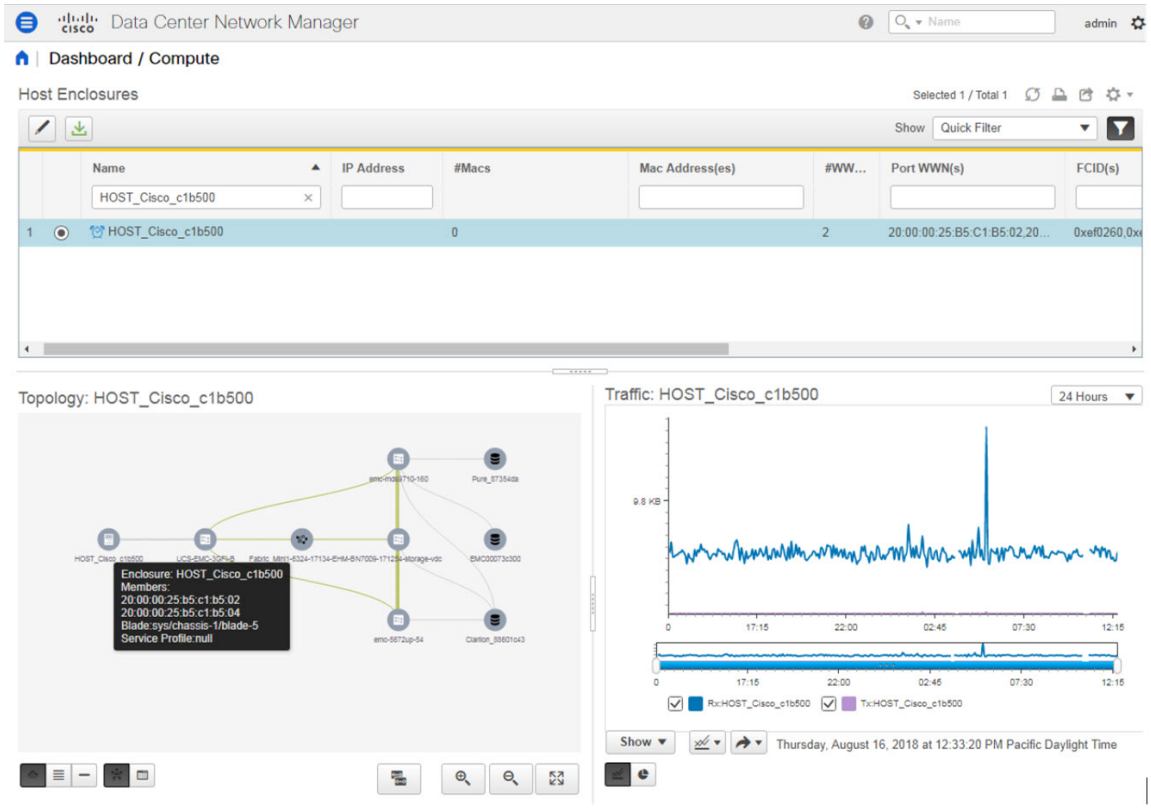

Data Center Network Manager
admin
Switches / UCSFI6332-17474-A (172.25.174.74)
System Info
Modules
Interfaces
License
Features
Blades
VHBA
VNIC
Port Capacity
24 Hour Traffic for Ether Port - sys/chassis-1/blade-8/adaptor-1/host-eth-1/eth-port-mcast-stats-rx
110
100
90
80
70
60
50
40
0
19:30
00:15
05:00
09:45
14:30
Time
Avg-mCast-Rx
Min-mCast-Rx
Max-mCast-Rx
Show
Monday, September 24, 2018 at 2:50:33 PM Pacific Daylight Time
Close
Total 14
Quick Filter
Discard RX
Avg
Min
Max
Unicast RX (packets)
4 sys/chassis-1/blade-8/adaptor-1 host-eth-2 0 0 0 0 0 0 0 0

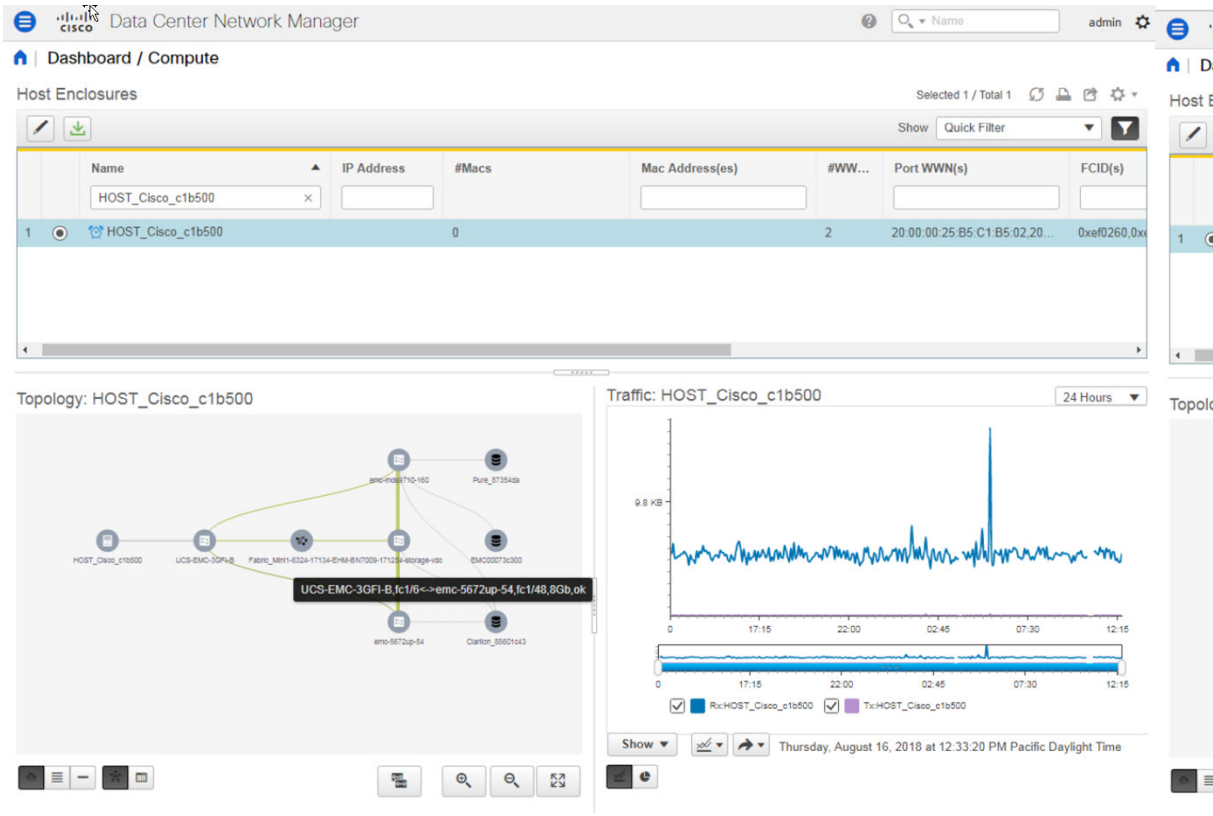
コンピューティング ダッシュボードで UCS FI 情報を表示

Cisco DCNM Web UI から、**[ダッシュボード（Dashboard）]>[コンピューティング（Compute）]** を選択します。

UCS FI に接続しているホスト エンクロージャの詳細をクリックして、トポロジ、サーバー ブレード情報、およびそのサービス プロファイルを表示します。

ブレードとサービス プロファイルの情報を表示するには、トポロジ内のホスト エンクロージャにカーソルを合わせます。





SMI-S ストレージの追加、編集、削除、再検出、更新

SMI-S プロバイダは、Cisco DCNM Web UI を使用して管理されます。

この項の内容は、次のとおりです。

SMI-S プロバイダーの追加

Cisco DCNM Web UI から SMI-S プロバイダを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）]** > **[検出（Discovery）]** > **[ストレージ デバイス（Storage Devices）]** を選択します。

[ストレージ デバイス（Storage Devices）] ウィンドウが表示されます。

ステップ 2 [SMI-S プロバイダの**追加**（Add SMI-S provider）] アイコンをクリックします。

[SMI-S プロバイダの追加（Add SMI-S Provider）] ウィンドウが表示されます。

ステップ 3 ドロップダウン リストを使用して、**[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。

Note SMS-S ストレージ検出用のデータ ソースを追加する前に、1 つの有効な DCNM 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 IP（SMI-S Server IP）]**、**[ユーザー名（Username）]**、および **[パスワード（Password）]** 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。

資格情報が検証され、有効な場合はストレージ検出が開始されます。資格情報チェックに失敗した場合は、有効な資格情報を入力するように求められます。

SMI-S プロバイダーの削除

Cisco DCNM Web UI から SMI-S プロバイダーを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [ストレージ デバイス（Storage Devices）]** を選択します。

ステップ 2 チェックボックスを使用して SMI-S プロバイダーを選択し、**[削除（Delete）]** アイコンをクリックします。

プロバイダーが削除され、プロバイダーに関連付けられているすべてのデータがシステムから削除されます。

SMI-S プロバイダの編集

Cisco DCNM Web UI から SMI-S プロバイダを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [ストレージ デバイス（Storage Devices）]** を選択します。

ステップ 2 チェックボックスを使用して SMI-S プロバイダを選択し、[SMI-S プロバイダの**編集（Edit SMI-S provider）]** アイコンをクリックします。

ステップ 3 **[SMI-S プロバイダの編集（Edit SMI-S Provider）]** ウィンドウで、ドロップダウンを使用して **[ベンダー（Vendor）]** を選択します。

ステップ 4 **[SMI-S サーバ IP（SMI-S Sever IP）]**、**[ユーザー名（User Name）]** および **[パスワード（Password）]** を指定します。

ステップ 5 **[名前スペース（Name Space）]** および **[Interop 名前スペース（Interop Name Space）]** を指定します。

ステップ 6 デフォルトでは、**ポート**番号が事前入力されています。

[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。

ステップ 7 **[適用 (Apply)]** をクリックします。

ストレージの検出が停止し、新しい情報を使用して新しいタスクが作成され、ストレージの検出が再開されます。

SMI-S プロバイダの再検出

Procedure

ステップ 1 **[インベントリ（Inventory）] > [検出（Discovery）] > [ストレージ デバイス（Storage Devices）]** を選択します。

ステップ 2 チェック ボックスを使用して SMI-S プロバイダを選択し、**[SMI-S プロバイダーの再検出（Rediscover SMI-S provider）]** をクリックします。

SMI-S プロバイダを消去

Procedure

ステップ 1 **[インベントリ > ディスカバリ > ストレージ デバイス（Inventory > Discovery > Storage Devices）]** を選択します。

ステップ 2 チェック ボックスを使用して SMI-S プロバイダーを選択し、**[パージ（Purge）]** をクリックします。

プロバイダがパージされます。

VMware サーバの追加、編集、再検出、削除

Cisco DCNM-SAN でサポートされている VMware サーバの Cisco DCNM-SAN でまとめられた Cisco DCNM レポート情報。

Note データソースに vCenter を追加する前に、 SAN が検出されていることを確認してください。

この項の内容は、次のとおりです。

VirtualCenter サーバーを追加

Cisco DCNM から仮想センター サーバを追加できます。

Procedure

ステップ 1 **[インベントリ > ディスカバリ > 仮想マシン マネージャ（Inventory > Discovery > Virtual Machine Manager）]** を選択。

Cisco DCNM-SAN によって管理されている VMware Server（存在する場合）のリストがテーブルに表示されます。

ステップ 2 [追加] をクリックします。

[vCenter の追加（Add VCenter）] ウィンドウが表示されます。

ステップ 3 この VMware **[VirtualCenter サーバー（Virtual Center Server）]** の IP アドレスを入力します。

ステップ 4 この VMware Server の**[ユーザ名（User Name）]**と**[パスワード（Password）]**を入力します。

ステップ 5 **[Add（追加）]** をクリックすると、このVMware Server の管理が開始されます。

VMware サーバを削除

Cisco DCNM から VMware サーバを削除できます。

Procedure

ステップ 1 **[インベントリ > ディスカバリ > 仮想マシン マネージャ（Inventory > Discovery > Virtual Machine Manager）]** を選択。

ステップ 2 VMware サーバのデータ収集を中止するために、削除したい VMware サーバの隣にあるチェック ボックスを選択して、**[削除（Delete）]** をクリックします。

VMware サーバーの編集

Cisco DCNM Web クライアントから VMware サーバーを編集できます。

Procedure

ステップ 1 **[インベントリ > 検出 > 仮想マシン マネージャ（Inventory > Discovery > Virtual Machine Manager）]** を選択します。

ステップ 2 編集する VMware サーバーの隣のチェックボックスをオンにして、**[Edit（編集）]** VirtualCenter アイコンをクリックします。

[vCenter の編集（Edit VCenter）] ダイアログ ボックスが表示されます。

ステップ 3 **[ユーザ名（User Name）]** と **[パスワード（Password）]** を入力します。

ステップ 4 管理対象または管理対象外のステータスを選択します。

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

VMware サーバの再検出

Cisco DCNM から VMware サーバを再検出できます。

Procedure

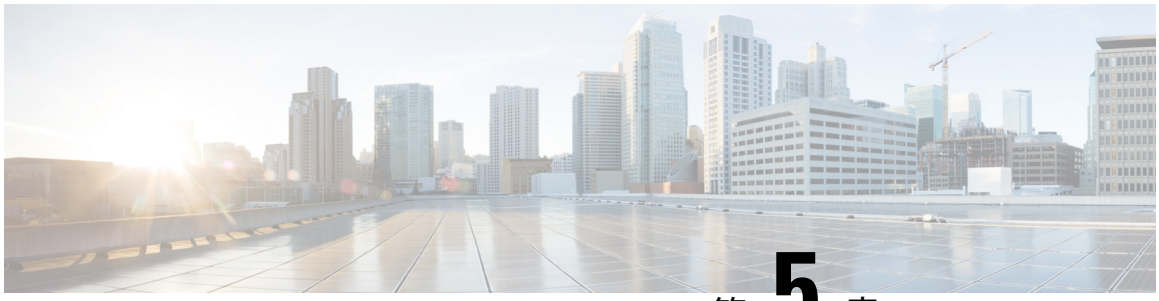
ステップ 1 **[インベントリ > 検出 > 仮想マシン マネージャ（Inventory > Discovery > Virtual Machine Manager）]** を選択します。

ステップ 2 再検出する VMware の隣のチェックボックスを選択します。

ステップ 3 **[再検出（Rediscover）]** をクリックします。

「再検出操作が完了するまでお待ちください」という警告が表示されたダイアログボックスが表示されます。

ステップ 4 ダイアログ ボックスで [OK] をクリックします。



第 5 章

モニター

この章は次のトピックで構成されています。

スイッチのモニタリング

[スイッチ（Switch）] メニューには次のサブメニューが含まれます。

スイッチ CPU 情報の表示

スイッチ CPU 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [CPU]** を選択します。

[CPU] ウィンドウが表示されます。このウィンドウには、その範囲内のスイッチの CPU 情報が表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタできます。

ステップ 3 **[スイッチ（Switch）]** 列でスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 4 **[スイッチ（Switch）]** 列のグラフ アイコンをクリックして、CPU 使用率を表示します。

また、チャートのタイムラインを の過去 10 分、過去 1 時間、前日、先週、先月、および昨年に変更することもできます。表示するグラフの種類とグラフのオプションも選択できます。

スイッチのメモリ情報の表示

スイッチ メモリ 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [メモリ（Memory）]** を選択します。

メモリー パネルが表示されます。このパネルには、その範囲内のスイッチの メモリ 情報が表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタ処理ができます。

ステップ 3 **[スイッチ（Switch）]** 列のグラフアイコンをクリックして、スイッチのメモリ使用量のグラフを表示します。

ステップ 4 **[スイッチ（Switch）]** 列でスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 5 ドロップダウンを使用して、さまざまなタイムラインでチャートを表示できます。チャートアイコンを使用して、さまざまなビューでメモリ使用チャートを表示します。

スイッチ トラフィックとエラー情報の表示

スイッチ トラフィックとエラー 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [Traffic（トラフィック）]** を選択します。

[スイッチ トラフィック（Switch Traffic）] パネルが表示されます。このパネルには、過去 24 時間のそのデバイスのトラフィックが表示されます。

ステップ 2 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します。

ステップ 3 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ます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 スイッチ名をクリックして、スイッチ ダッシュボード セクションを表示します。

スイッチ温度の表示

Cisco DCNM には、スイッチのセンサー温度を表示できるモジュール温度センサー モニタリング機能が含まれています。センサー リストをフィルタ処理する間隔を選択できます。デフォルトの間隔は **[最終日（Last Day）]** です。履歴温度データを持つセンサーのみがリストに表示されます。過去 10 分間、過去 1 時間、最終日、先週、および先月から選択できます。

Note **[構成（Configure）] > [資格情報管理（Credentials Management）] > [ローカル エリア ネットワーク資格情報（LAN Credentials）]** 画面で LAN または SAN の資格情報を設定して、スイッチから温度モニタリング データを取得する必要はありません。

スイッチ 温度情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [温度（Temperature）]** を選択します。

[スイッチ温度（Switch Temperature）] ウィンドウには、次の列が表示されます。

- **[範囲（Scope）]**: センサーは、ファブリックの一部であるスイッチに属しています。属しているファブリックが範囲として表示されます。Cisco DCNM の上部にある範囲 セレクタを使用すると、センサー リストはその範囲によってフィルタ処理されます。
- **[スイッチ（Switch）]** : センサーが属するスイッチの名前。
- **[IP Address（ IP アドレス ）]** : スイッチの IP アドレス。
- **[温度モジュール（Temperature Module）]** : センサー モジュールの名前。
- **[平均 / 範囲（Avg/Range）]** : 最初の数値は、表の上部で指定された間隔での平均温度です。2 番目の数値セットは、その間隔における温度の範囲です。
- **[ピーク（Peak）]** : インターバルにおける最高温度

ステップ 2 このリストの各行には、クリックできるチャート アイコンがあります。
センサーの履歴データを示すチャートが表示されます。このチャートの間隔も 24 時間、1 週間あるいは1 か月の間で変更できます。

温度監視の有効化

ローカル エリア ネットワーク（LAN）コレクション画面からローカル エリア ネットワーク（LAN）スイッチの温度モニタリング機能を有効にできます。また、[管理] > [DCNM サーバ] >[サーバプロパティ] 画面でいくつかのプロパティを設定することで、SAN スイッチの温度モニタリング機能を有効にすることができます。

SAN スイッチの温度モニタリングの有効化

1. **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** をメニュー バーから選択します。
2. **# PERFORMANCE MANAGER > COLLECTIONS** エリアに移動します。
3. 環境フィールド **pm.collectSanTemperature** および **pm.sanSensorDiscovery** を **TRU**E に設定します。
4. **[変更を適用（Apply Changes）]** をクリックして構成に変更を適用します。
5. Cisco DCNM を再起動します。

その他の統計情報の表示

Cisco DCNM Web UI からユーザー定義フォーマットで統計を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [切り替え（Switch）] > [ユーザー定義（User Defined）]** を選択します。

[その他（Other）] ウィンドウが表示されます。

ステップ 2 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。

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、次のことを実行することもできます。

- 時間範囲を選択して**[フィルタ（Filter）]**をクリックすると、表示がフィルタ処理されます。
- **[スイッチ（Switch）]**列のチャートアイコンをクリックして、このユーザー定義オブジェクトのパフォーマンスのグラフを表示します。時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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。

スイッチのカスタム ポート グループ情報の表示

Cisco DCNM Web UI からカスタム ポート グループ情報を表示するために、次の手順を実行します。

手順

ステップ 1 **[モニタ（Monitor）]>[スイッチ（Switch）]>[カスタム ポート グループ（Custom Port Group）]** を選択します。

[カスタム ポート グループ（Custom Port Groups）] ウィンドウには、カスタム ポート グループの統計とパフォーマンスの詳細が表示されます。

ステップ 2 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。

ステップ 3 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ます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 スイッチ名をクリックして、スイッチ ダッシュボードを表示します。

アカウンティング情報の表示

アカウンティング情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ] > [スイッチ] > [アカウンティング]**の順に選択します。

アカウンティング情報とともにファブリック名またはグループ名が表示されます。

ステップ 2 アカウンティング情報を **[送信元（Source）]** 、 **[ユーザー名（Username）]** 、**[時間（Time）]** と **[詳細（Description）]** で検索するためにフィルタ アイコンの横にある **[高度フィルタ（Advanced Filter）]** を選択ます。 または **[クイック フィルタ（Quick Filter）]** カラムの元で検索するために選択します。

ステップ 3 行を選択して **[削除（Delete）]** アイコンをクリックすることによってリストのアカウンティング情報を削除することもできます。

ステップ 4 **[印刷（Print）]**アイコンを使用してアカウンティングの詳細を印刷し、**[エクスポート（Export）]** アイコンを使用してデータを Microsoft Excel スプレッドシートにエクスポートできます。

イベント情報の表示

Cisco DCNM Web UI からイベントと syslog を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [Events（イベント）]** を選択します。

ファブリック、スイッチ名、およびイベントの詳細が表示されます。

[数（Count）] 列には、**[最後に見た（Last Seen）]** および **[最初に見た（First Seen）]** 列に示されているように、期間中に同じイベントが発生した回数が表示されます。

[スイッチ（Switch）] 列のスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 2 テーブルでイベントを選択し、**[サプレッサーの追加（Add Suppressor）]** アイコンをクリックして、イベント サプレッサー ルールを追加するショートカットを開きます。

ステップ 3 テーブルから 1 つ以上のイベントを選択し、**[確認（Acknowledge）]** アイコンをクリックして、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の横の **Ack** 列に表示されます。

ステップ 4 ファブリックを選択し、**[未確認（Unacknowledge）]** アイコンをクリックして、ファブリックの確認をキャンセルします。

ステップ 5 アカウンティング情報を **[送信元（Source）]** 、 **[ユーザー名（Username）]** 、**[時間（Time）]** と **[詳細（Description）]** で検索するためにフィルタ アイコンの横にある **[高度フィルタ（Advanced Filter）]** を選択します。 または **[クイック フィルタ（Quick Filter）]** カラムの元で検索するために選択します。

ステップ 6 ファブリックを選択し、**[削除（Delete）]** アイコンを使用して、リストからファブリックおよびイベント情報を削除します。

ステップ 7 イベント情報を印刷するには **[印刷（Print）]** アイコンをクリックします。

ステップ 8 **[Excel にエクスポート（Export to Excel）]** アイコンをクリックして、データをエクスポートします。

SAN のモニタリング

SAN メニューには次のサブメニューが含まれます。

ISL トラフィックとエラーのモニタリング

Cisco DCNM Web UI から ISL トラフィックとエラーをモニタするには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [SAN] > [ISL]** を選択します。

[ISL トラフィックとエラー（ISL Traffic and Errors）] ウィンドウが表示されます。このパネルには、その範囲内のエンドデバイスの ISL 情報が表示されます。範囲メニューを使用して、表示される範囲を縮小または拡大できます。

ステップ 2 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。

Note データ グリッドの **NaN** (非数) は、データが利用できないことを意味します。

Note **[FCIP 圧縮率（FCIP Compression Ratio）]**列の下の非 FCIP ポートの場合は空です。

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 ISL の詳細情報を表示することもできます。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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。リアルタイム情報を表示するには、右上隅の **[更新（Refresh）]** アイコンを選択します。リアルタイム データは 10 秒ごとに更新されます。
- 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。
- Rx/Tx の計算については、以下の Rx/Tx 計算式を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

パフォーマンステーブルにデータが含まれていない場合は、パフォーマンス設定のしきい値セクションを参照してパフォーマンスをオンにします。

NPV リンクのパフォーマンス情報の表示

Cisco DCNM Web UI から NPV リンクのパフォーマンスを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [SAN] > [NPV リンク（NPV Links）]** を選択します。

[NPV リンク（NPV Links）] ウィンドウが表示されます。このウィンドウには、選択したスコープの NPV リンクが表示されます。

ステップ 2 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。

ステップ 3 **[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。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データの収集をオンにするため、セクション パフォーマンス セットアップのしきい値, on page 360 を参照してください。

VSAN のインベントリ情報の表示

Cisco DCNM Web UI の VSAN 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

[モニタ] > [SAN] > [VSAN] を選択します。

VSAN ウィンドウが表示され、VSAN の詳細がステータスおよび**アクティブ化されたゾーンセット**の詳細とともに表示されます。

イーサネットポートに関するパフォーマンス情報のモニタリング

Cisco DCNM Web UI からイーサネット ポートのパフォーマンスをモニタリングするには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ]** > **[SAN]** > **[ポート]** を選択します。

[イーサネット ポート（Ethernet Ports）] ウィンドウが表示されます。

ステップ 2 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。

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、次の手順を実行することもできます。

- **[名前（Name）]** 列のイーサネット ポートを選択し、過去 24 時間のイーサネット ポート上のトラフィック図を表示します。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時間範囲を選択します。
- 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。
- 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。
- Rx/Tx の計算については、以下の Rx/Tx 計算式を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データの収集をオンにするため、セクション パフォーマンス セットアップのしきい値, on page 360 を参照してください。

FC エンド デバイスにあるホスト ポートのインベントリ情報の表示

Cisco DCNM Web UI から FC エンド デバイスのホスト ポート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 **[モニタ（Monitor）] > [SAN] > [FC ポート（FC Ports）]** を選択します。

[インベントリ（Inventory）] > [エンド ポート（End Ports）] ウィンドウが表示され、ホスト ポート上の FC エンド デバイスの詳細が示されます。

ステップ 2 ドロップダウンを使用して、ホスト ポート上の FC エンド デバイスのすべてまたは警告情報を表示します。

ステップ 3 **[フィルタを表示（Show Filter）]** アイコンをクリックして、**[エンクロージャ、デバイス名（Enclosure, Device Name）]**、または **VSAN** によるフィルタリングを有効にします。

すべてのポートに関するパフォーマンス情報の表示

Cisco DCNM Web UI からすべてのポートに接続されているデバイスのパフォーマンスを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[パフォーマンス（Performance）] > [エンド デバイス（End Devices）]** を選択します。

[エンド デバイス トラフィックおよびエラー（End Devices Traffic and Errors）] ウィンドウが表示されます。

ステップ 2 右上隅のドロップダウン リストから、**[すべて（All）]** のポート、**[ホスト（Host）]** ポート、または **[ストレージ（Storage）]** ポートの表示を選択できます。

ステップ 3 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。

ステップ 4 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。

ステップ 5 **[名前（Name）]** 列のグラフ アイコンをクリックして、次を表示します。

- 選択されたタイムラインに従ったデバイス上のトラフィックのグラフ
- 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。リアルタイム情報を表示するには、右上隅のドロップダウン リストから更新アイコンをクリックします。リアルタイム データは 10 秒ごとに更新されます。アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[データの補間（Interpolate Data）]** することもできます。

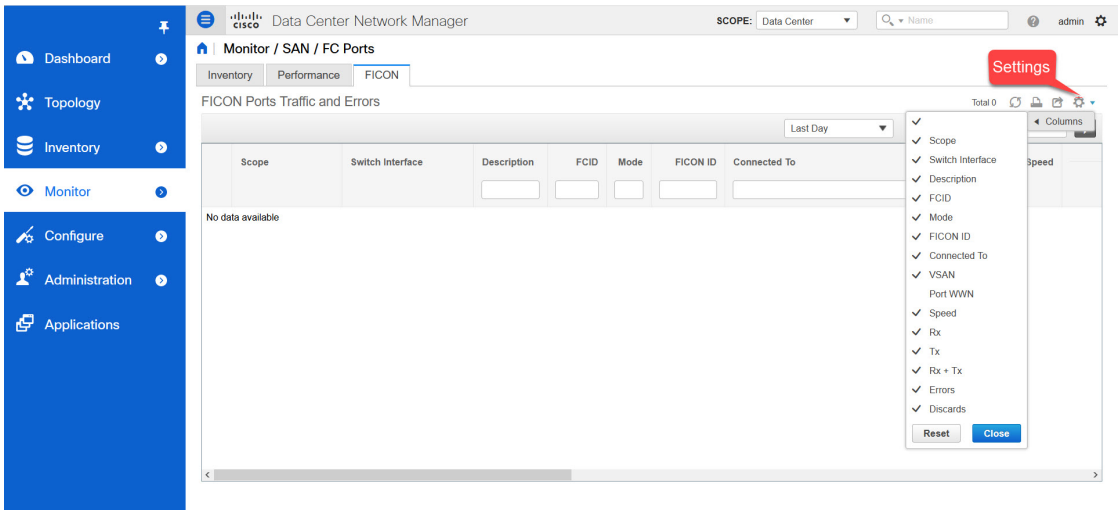
Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、セクション パフォーマンス セットアップのしきい値, on page 360 を参照してください。

FICON ポートの表示

次の表は、すべての FICON ポートのトラフィックとエラー情報を示しています。

フィールド	説明
範囲	FICON ポートを持つファブリック範囲を指定します。
スイッチ インターフェイス	[チャートの表示（Show Chart）]アイコンをクリックして、選択したスイッチインターフェイスのポート トラフィックを表示します。
説明	FICON ポートの説明を指定します。
FCID	ファイバ チャネル ID を指定します。
モード	ポートのタイプを指定します。有効な値は**CH** と **CU** です。値は、FICON チャネルの場合は CH、FICON 制御ユニットの場合は CU です。
FICON ID	FICON ポート ID を指定します。
接続先	FICON ポートが接続されているデバイスを指定します。
VSAN	VSAN ID を指定します。
スピード	FICON ポートの速度を指定します。
Rx	平均およびピークの Rx トラフィックを指定します。
Tx	平均およびピークの Tx トラフィックを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー	平均およびピークの入出力エラーを指定します。
破棄	平均およびピークの入力および出力廃棄を指定します。

[設定（Settings）] > [列（Columns）] を選択し、ドロップダウン リストから **[ポート WWN（Port WWN）]** オプションを選択すると、ポート WWN の詳細を表示できます。



印刷、データのエクスポート、または表示したい列のカスタマイズを行うことができます。テーブルを更新して最新のデータを確認します

Cisco DCNM Web UI から FICON ポートのトラフィックとエラーを表示するには、次の手順を実行します。

手順

ステップ 1 **[モニタ（Monitor）] > [SAN] > [FC ポート（FC Ports）]** を選択します。

[インベントリ（Inventory）] ウィンドウが表示されます。

ステップ 2 **[FICON]** タブをクリックします。

ステップ 3 トラフィックを表示するスイッチ インターフェイスの **[チャートの表示（Show Chart）]** アイコンをクリックします。

リアルタイムデータは10秒ごとに更新されます。アイコンを使用して、データを追加、予測、および補間することもできます。

（注） **[欠損データを補間しない（Do Not interpolate Missing Data）]** アイコンをクリックして、チャート内の欠損データのギャップを削除します。デフォルトでは、欠損データはすべてのチャートで補間されます。

トラフィックの表示方法を選択できます。期間、形式に基づいてトラフィックの詳細を表示し、この情報をエクスポートできます。

[期間（Duration）] ドロップダウンリストでは、次のオプションを選択できます。

- 24時間
- 週
- 月
- 年

表示 : **[表示（Show）]** をクリックし、ドロップダウン リストから **[チャート（Chart）]**、**[表（Table）]**、または **[チャートと表（Chart and Table）]** を選択して、トラフィックの詳細を表示する方法を表示します。

[チャート（Chart）] を選択した場合、トラフィック チャートにカーソルを合わせると、Y 軸に沿って、対応する時間の Rx 値と Tx 値が X 軸に沿って表示されます。時間範囲セレクターのスライダを動かすことで、X 軸の持続時間の値を変更できます。Rx および Tx チェック ボックスをオンまたはオフにして、Y 軸の値を選択できます。

（注） 期間として**週**、**月**、または**年**を選択すると、Y 軸に沿ってピーク受信およびピーク送信の値を表示することもできます。

[表（Table）] を選択して、交通情報を表形式で表示します。

チャートの種類と**チャートのオプション** : **[チャートの種類（Chart Type）]** ドロップダウン リストから**面チャート**または**線チャート**を選択します。

[塗りつぶしパターンを表示（Show Fill Patterns）] チャート オプションを選択できます。

アクション : **[アクション（Actions）]** ドロップダウン リストから適切なオプションを選択して、トラフィック情報をエクスポートまたは印刷します。

FC フローのパフォーマンス情報の表示

Cisco DCNM Web UI から FC フロー トラフィックのパフォーマンスを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [SAN] > [FC フロー（ FC Flows）]** を選択します。

[FC フロー（FC Flow）] ウィンドウが表示されます。

ステップ 2 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。

ステップ 3 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。

ステップ 4 **[名前（Name）]** 列のチャート アイコンをクリックして、以下を表示します。

- 選択されたタイムラインに従ったデバイス上のトラフィックのグラフ
- 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。リアルタイム情報を表示するには、右上隅のドロップダウンリストから**[更新（Refresh）]** アイコンをクリックします。
- アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[データの補間（Interpolate Data）]** することもできます。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、セクションパフォーマンス セットアップのしきい値, on page 360 を参照してください。

エンクロージャのパフォーマンス情報

Cisco DCNM Web UI からホスト エンクロージャに接続されているデバイスのパフォーマンスを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [SAN] > [エンクロージャ（Enclosures）]** を選択します。

[エンクロージャ トラフィックおよびエラー（Enclosures Traffic and Errors）] ウィンドウが表示されます。

ステップ 2 右上隅のドロップダウン リストから、表示する**[ホスト エンクロージャ（Host Enclosures）]**または**[ストレージ エンクロージャ（Storage Enclosures）]**を選択できます。

ステップ 3 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。

ステップ 4 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。

ステップ 5 **[名前（Name）]** 列のチャート アイコンをクリックして、以下を表示します。

- 選択されたタイムラインに従ったデバイス上のトラフィックのグラフ
- 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 **[データの補間（Interpolate Data）]** することもできます。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、セクションパフォーマンス セットアップのしきい値, on page 360 を参照してください。

ポート グループに関するパフォーマンス情報の表示

Cisco DCNM Web UI からポート グループに接続されているデバイスのパフォーマンスを表示するには、次の手順を実行します：

Procedure

ステップ 1 **[モニタ（Monitor）] > [SAN] > [ポート グループ（Port Group）]** を選択します。

[ポート グループトラフィックとエラー（Port Group Traffic and Errors）] ウィンドウが表示されます。

ステップ 2 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。

ステップ 3 ポート グループの名前をクリックして、そのポート グループのメンバーを表示します。

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ポート グループの詳細情報を表示することもできます。

- 時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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 **[データの補間（Interpolate Data）]** 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。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、セクションパフォーマンス セットアップのしきい値, on page 360 を参照してください。

SAN ホストの冗長性

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。

Note 検出されたすべてのファブリックはライセンス付与する必要があります。そうしない場合は、この機能は Cisco DCNM Web Client 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。

ホスト パスの冗長性は、DCNM に表示されるエンクロージャ名を使用して、ポートが同じエンクロージャの一部であると判断します。エンクロージャ名が完全に同じでない場合、それらは別個のデバイスとして表示されます。名前が完全に同じでない場合、ホスト パスの冗長性と他の機能がそれらを同じデバイスと見なすために、ユーザーは DCNM のエンクロージャの編集ダイアログで名前を手動で変更する必要があります。

メニュー バーから、**[モニタ（Monitor）] > [SAN] > [ホスト パスの冗長性（Host Path Redundancy）]** を選択します。

このウィンドウには 2 つの部分が表示されます。

実行テスト

Procedure

ステップ 1 **[モニタ（Moniter）] > [SAN] > [ホストパスの冗長性（Host Path Redundancy）]** を選択します。

ステップ 2 上にある**[実行テスト（Test to Run）]** エリアで、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 時間ごとにチェックを自動的に実行する（Automatically Run Check 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 下にある成果の領域に結果が表示されます。

成果

Procedure

ステップ 1 **[モニタ（Moniter）] > [SAN] > [ホストパスの冗長性（Host Path Redundancy）]** タブを選択します。

ステップ 2 **[下部の結果（Results）]**エリアには、**[ホスト パス エラー（Host Path Errors）]**、**[無視されたホスト（Ignored Hosts）]**、**[無視されたストレージ（Ignored Storage）]**、**[および無視されたホスト ストレージ ペア（Ignored Host Storage Pairs）]**の 4 つのタブがあります。

ステップ 3 **[ホストパスエラー（Hostpath Errors）]** タブをクリックして、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、色付きの**[良好、スキップ（Good, Skipped）]** と **[エラー（Errored）]** ホストのエンクロージャの数と最終アップデート時間が表示されます。

a) **[ホスト エンクロージャ（Host Enclosure）]**列には、エラーを含むホストが表示されます。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 エンクロージャー/ストレージ ポート（Storage Enclosure/Storage Port）]** 列には、エラーに関連する接続されたストレージが表示されます。**[修正？（Fix?）]**列で、マウス カーソルを **?** に合わせます。アイコンをクリックして、エラーを修正するソリューションを表示します。

b) 行をクリックし、**[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。

c) 行をクリックし、**[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。

d) 行をクリックし、**[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。

e) 表の右上隅にある **[表示（Show）]** の横にあるドロップダウン リストで、**[クイック フィルタ処理（Quick Filter）]** を選択します。表の列ヘッダーにキーワードを入力して、項目をフィルタ処理します。**[すべて（All）]**を選択すると、すべての項目が表示されます。

f) 表の右上隅にある循環アイコンをクリックして、表を更新します。

g) エラーとテーブルを印刷するには、テーブルの右上隅の **[印刷（Print）]** アイコンをクリックします。

h) テーブルの右上隅にある **[エクスポート（Export）]** アイコンをクリックして、テーブルを Microsoft Excel スプレッドシートにエクスポートします。

ステップ 4 **[無視されたホスト（Ignored Host）]** タブをクリックして、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の理由とともに表示します。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.）]

ホストエンクロージャを選択し、**[削除（Delete）]** 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。ただし、**[ホストがユーザーによって無視されました（Host was ignored by user）]**というメッセージが表示されたエントリを削除することはできます。

ステップ 5 **[無視されたストレージ（Ignored Storage）]** タブをクリックして、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。ストレージエンクロージャを選択し、**[削除（Delete）]** 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。

ステップ 6 **[無視されたホストストレージペア（Ignored Host Storage Pair）]** タブをクリックして、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。行を選択し、**[削除（Delete）]** をクリックして、無視されたリストからストレージ ペアを削除します。

低速ドレイン分析

低速ドレイン分析では、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。

低速ドレイン統計は、キャッシュメモリに保存されています。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。

ビデオを見て、SAN Insights を使用して、Cisco DCNM を使用してファブリック全体で低速ドレイン メトリックが増加しているかどうかを識別する方法を示すこともできます。ビデオ: SAN Insights による低速ドレイン分析を参照してください。

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 **[モニタ] > [SAN] > [低速ドレイン分析（Slow Drain Analysis）]** を選択します。

ステップ 2 **[範囲（Scope）]** フィールドで、ドロップダウン リストからファブリックを選択します。

ステップ 3 **[期間（Duration）]** ドロップダウンリストで、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）]** には、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。

[毎日（Daily）] の低速ドレイン ジョブのみがレポートを送信し、ます。レポートは、**[モニタ（Monitor）] > [レポート（Report）] > [表示（View）]** から表示できます。

ステップ 4 **[収集の開始（Start Collection）]** をクリックして、投票を開始します。

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 5 **[収集の停止（Stop Collection）]** をクリックして、投票を停止します。

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 6 **[現在のジョブ（Current jobs）]** の横にある矢印をクリックして、ファブリックで実行されているジョブの低速ドレインの詳細を表示します。各ファブリックの **[ファブリック名（Fabric Name）]**、[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 7 ファブリックを選択し、**[結果（Result）]**、**[削除（Delete）]** または **[停止（Stop）]** をクリックしてジョブを表示、削除、停止します。

ファブリックを選択して **[結果（Result）]** をクリックすると、選択したファブリックのトポロジが低速ドレインの詳細とともに表示されます。詳細については、「低速ドレインの視覚化」を参照してください。

ステップ 8 **[詳細（Detail）]**をクリックして、保存された情報を表示します。

ステップ 9 **[インターフェイス チャート（Interface chart）]**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。

ステップ 10 **[フィルタ処理（Filter）]** をクリックして、各列に定義された値に基づいて詳細を表示します

ステップ 11 **[データ行のみ（Data Rows Only）]** チェックボックスを選択し、0 ではないエントリをフィルタし表示します。

ステップ 12 **[印刷（Print）]** をクリックして、低速ドレインの詳細を印刷します。

ステップ 13 **[エクスポート（Export）]** をクリックして、低速ドレインの統計を Microsoft Excel スプレッドシートにエクスポートします。

低速ドレインの可視化

ファブリックを選択して **[結果（Result）]** をクリックすると、選択したファブリックのトポロジが、低速ドレインの詳細とともに表示されます。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の一部を取得できます。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、トポロジの低速ドレイン情報を表示します。**[管理（Administration）]** > **[パフォーマンス セットアップ（Performance Setup）]** > **[SAN コレクション（SAN Collections）]** を選択してパフォーマンス コレクションを有効にします。パフォーマンス コレクションを有効にする方法の詳細については、Performance Manager SAN 収集, on page 360 を参照してください。**[管理（Administration）]** > **[イベント設定（Event Setup）]** > **[登録（Registration）]** を選択し、SNMP トラップを有効にします。SNMP トラップを有効にする方法の詳細については、 #unique_144を参照してください。

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 9: **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	低速ドレイン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%
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低速ドレインを表します。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、低速ドレインが発生している 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低速ドレインを表します。スイッチをクリックすると、低速ドレインの詳細が表示されます。スイッチをダブルクリックして低速ドレイン表をフィルタ処理し、そのスイッチのみの低速ドレイン データを表示します。

リンクの低速ドレインを表すために、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、低速ドレイン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。リンクをダブルクリックして低速ドレイン表をフィルタ処理し、そのリンクのみに関連する低速ドレインデータを表示します。

Note リンクが持つことができる最高の低速ドレイン 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。

標準ゾーンに関するインベントリ情報の表示

Cisco DCNM Web UI から通常ゾーン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 **[モニタ（Monitor）] > [SAN] > [通常ゾーン（Regular Zones）]** を選択します。

[通常ゾーン（Regular Zones）] ウィンドウが表示されます。

ステップ 2 表示されている列を選択するために **[設定（Settings）]** アイコンをクリックします。

What to do next

Cisco DCNM リリース 11.4(1) 以降、ゾーン移行ツールを使用して、pWWN ベースの SAN ゾーンを Brocade スイッチから Cisco MDS スイッチに移行できます。

この機能は、このリリースの Brocade Fabric OS v7.xx 以降を実行している Brocade のファブリック スイッチの移行をサポートします。

ゾーン移行ツール

Cisco DCNM リリース 11.4(1) 以降、pWWN ベースの SAN ゾーンを Brocade スイッチから Cisco MDS スイッチに移行できます。これには、次の手順が含まれます。

1. Brocade 構成ファイルの生成
2. ゾーン移行ツールを使用した構成ファイルの移行
3. Cisco MDS スイッチでのゾーニング出力の適用

この機能は、このリリースの Brocade Fabric OS v7.xx 以降を実行している Brocade のファブリック スイッチの移行をサポートします。

Brocade 構成ファイルの生成

Cisco DCNM を使用して Brocade SAN ゾーンを Cisco MDS スイッチに移行する前に、Brocade 構成ファイルを生成します。

次のいずれかのオプションを使用して、Brocade 構成ファイルを生成できます。

- CLI の使用: admin または管理アクセス権を持つ同等のロールを使用して、Brocade スイッチ ターミナルにログインします。**cfgshow** コマンドを実行します。コマンド出力をテキスト ファイルにコピーして保存します。
- Brocade Fabric OS Web ツールの使用：**[スイッチ管理（Switch Administration）]** ウィンドウから **[ゾーニング情報（Zoning Information）]** ファイルをダウンロードします。詳細については、『*Brocade* ファブリック *OS Web* ツール管理ガイド』の「スイッチ レポートの表示および印刷」セクションを参照してください。

ゾーン移行ツールを使用した構成ファイルの移行

Cisco DCNM を使用して Brocade 設定ファイルを変換するには、Cisco DCNM Web UI から次の手順を実行します。

手順

ステップ 1 **[モニタ（Monitor）] > [SAN] > [通常ゾーン（Regular Zones）]** を選択します。

ステップ 2 **[ゾーン移行ツール]** ボタンをクリックします。

[ゾーン移行ツール] ダイアログボックスが表示されます。

ステップ 3 **[入力ファイルの選択]** をクリックして、システムから Brocade 構成ファイルを選択します。

ステップ 4 ゾーンを追加する必要がある VSAN 番号を入力します。

有効範囲は 1 ～ 4093 です。

ステップ 5 （オプション）**[拡張ゾーン モード（Enhanced Zone Mode）]** または **[拡張デバイス エイリアス モード（Enhanced Device-Alias Mode）]** チェック ボックスをオンにします。

（注） 拡張ゾーン モードと拡張デバイス エイリアス モードの利点を確認するには、『*Cisco MDS 9000* ファブリック構成ガイド』の「ゾーンの構成と管理」の章と「デバイス エイリアス サービスの配布」の章を参照してください。

ステップ 6 **[変換（Convert）]** をクリックし、変換を開始します。

エラーがない場合、変換されたファイルはローカル システムにダウンロードされます。

（注）
- ハード ゾーンまたはインターフェイス ベースのゾーンを変換しようとすると、エラーが発生します。
- 2000 を超える fcAlias ゾーンを Brocade から Cisco MDS に移行しようとすると、それらはデバイス エイリアス ゾーンに変換されます。

次のタスク

ダウンロードしたファイルを Cisco MDS スイッチで実行します。

Cisco MDS スイッチでのゾーニング出力の適用

Brocade 構成ファイルを Cisco MDS スイッチと互換性のある形式に変換したら、それらを Cisco MDS スイッチに適用します。

出力を Cisco MDS スイッチに適用するには、次の手順を実行します。

手順

ステップ 1 Cisco MDS スイッチ コンソールにログインします。

ステップ 2 テキストエディタを使用して変換したファイルを開きます。

ステップ 3 テキストエディタを使用して変換したファイルを開きます。

ステップ 4 **copy running-config startup-config**コマンドを使用して構成を保存します。

ゾーンは Cisco MDS スイッチに移行されます。

IVR ゾーンに関するインベントリ情報の表示

Cisco DCNM Web UI の IVR ゾーン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 **[モニタ > SAN > IVR ゾーン（Monitor > SAN > IVR Zones）]** を選択します。

[IVR ゾーン（IVR Zones）] ウィンドウに、IVR ゾーンのファブリックのインベントリの詳細が表示されます。

ステップ 2 表示されているカラムを選択するために **[設定（Settings）]** アイコンをクリックします。

Insights フローのモニタリング

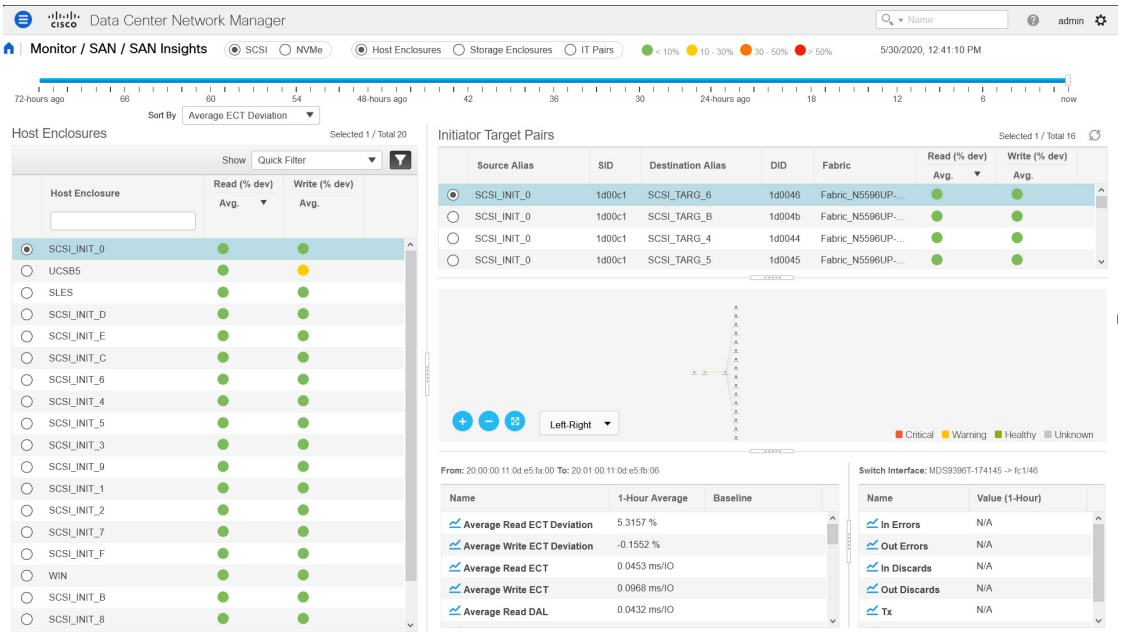
[SAN Insights（SAN Insights）] ページには、環境内の問題をすばやく特定できるように、インターフェイスにヘルス関連のインジケータが表示されます。ヘルスインジケータを使用して、ファブリックのどこに問題があるかを理解できます。

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

Note インターフェイスがダウンしている場合は、灰色で表示されます。

Procedure

ステップ 1 SAN Insights 機能をモニタリングするには、**[モニター（Monitor）] > [SAN] > [SAN Insights]** を選択します。SAN Insights ページが表示されます。



このページは、カウンター データを表示する Insights データの視覚化、マップ上のインジケーターを備えた視覚的なトポロジマップの基礎を提供します。また、分析情報と過去のインサイトを表示することもできます。Cisco DCNM リリース 11.3(1) 以降、データ タイプを選択して SAN Insights データをストリーミングできます。**SCSI** または **NVMe** を選択して、データ タイプを選択します。ウィンドウの右隅にシステム時刻が表示されます。

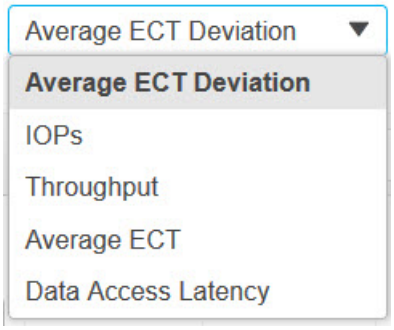
[モニタ（Monitor）] > [SAN Insights] ウィンドウでは、以下の手順で説明されているタスクを実行できます。

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。

Note 赤いステータス ボールをクリックして、イニシエータ-ターゲット ペア テーブルの**読み取り（% dev）**または**ライター（% dev）**列の下にある **SAN Insights メトリクス**を表示し、それぞれのイニシエータ-ターゲット ペアの詳細については、ECT 分析ページに移動します。

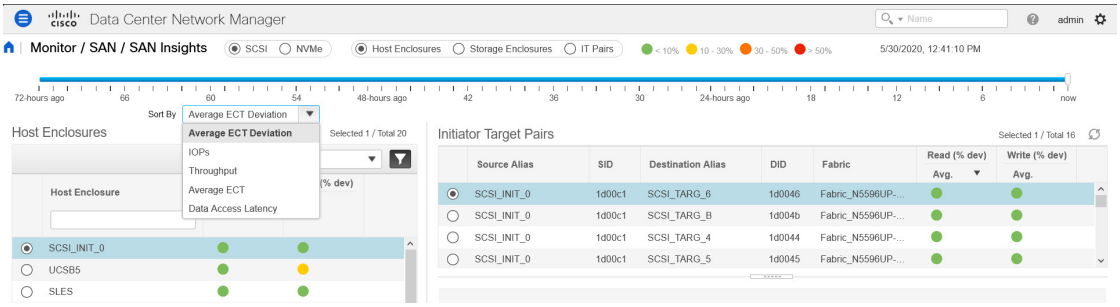
ステップ 2 **ホスト エンクロージャ、ストレージ エンクロージャ、**または**IT ペア**に関する詳細を表示します。

以下の図に示すように、平均値に基づいてエンクロージャの詳細を表示することを選択できます。ホスト エンクロージャ、ストレージ エンクロージャ、または IT ペアは、クイック フィルタ機能を使用してフィルタ処理できます。

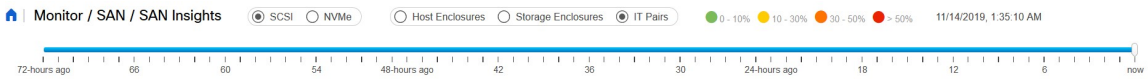


デフォルトでは、フィルタ タイプの **[平均 ECT 偏差]** が選択されています。イニシエータ ターゲット ペアには、読み取りおよび書き込み偏差のステータスが色付きのステータス ボールとして表示され、クリックして SAN Insights メトリックを表示できます。ただし、他のすべてのフィルタ タイプでは、読み取りおよび書き込みのパーセンテージ偏差のステータスが数値形式で表示されます。

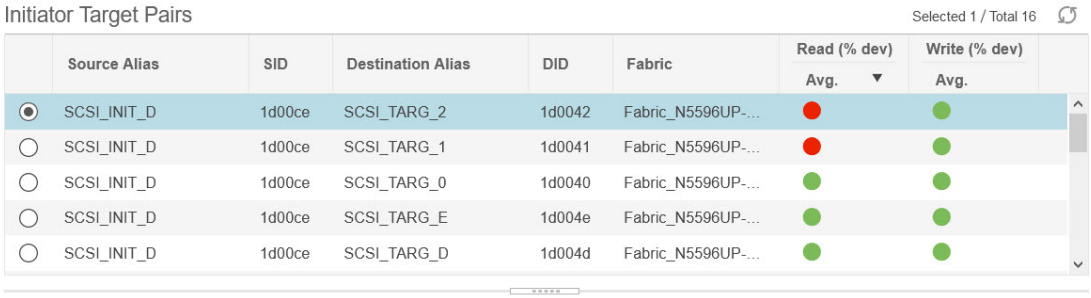
フィルタリングされたメトリックの読み取り/書き込み操作によって、エンクロージャ/IT ペアを並べ替えることができます。並べ替えを変更するには、列ヘッダをクリックします。デフォルトでは、読み取り操作でソートされています。



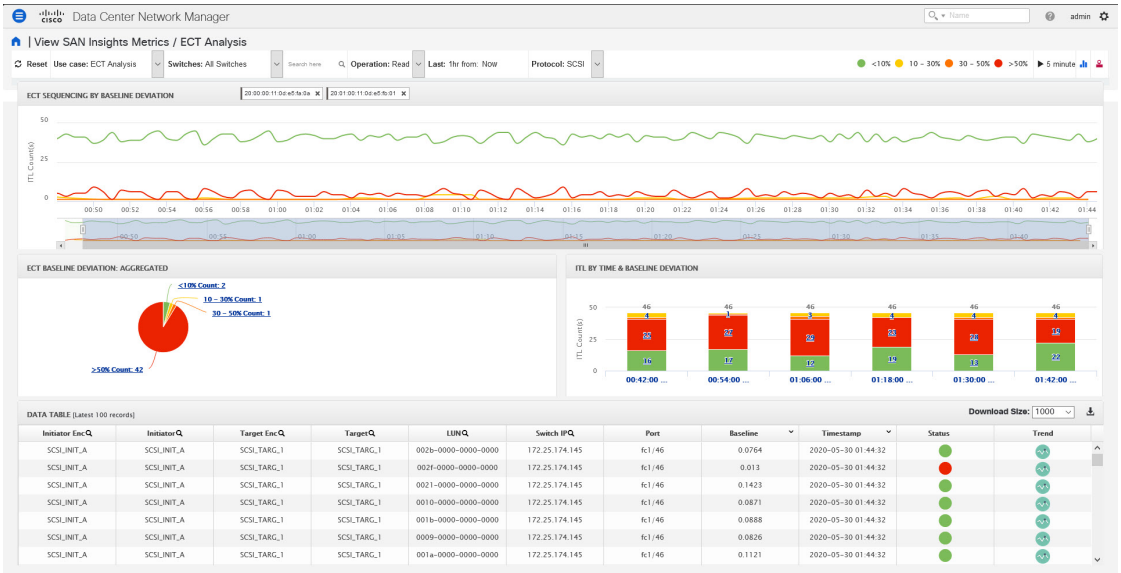
ステップ 3 時間間隔（現在、6時間前、12時間前など）を選択して、ステータスを計算し、フローとポートのカウンタを取得します。



ステップ 4 選択したエンクロージャごとに、送信元エイリアス、SID、接続先エイリアス、DID、ファブリック名、読み取り（% dev）、ライター（% dev）などのイニシエータ ターゲット ペアの詳細を表示します。



[イニシエータとターゲットのペア] テーブルの **[読み取り（% dev）]** または **[ライター（% dev）]** 列の下にあるステータス サークル アイコンをクリックして、対応するイニシエータとターゲットの WWPN が事前にフィルタ処理された状態で、ECT 分析ウィンドウに移動できます。



ステップ 5 マップを使用して、イニシエータからターゲットへのエンドツーエンドの接続を表示します。ホスト、ストレージ、およびスイッチには、色付きのステータス表示があります。トポロジエリアのカラーコードは、スイッチのステータス専用です。スイッチの色は、スイッチごとに計算されたヘルス スコアによって管理されます。詳細については、色付きのスイッチ アイコンをダブルクリックして、スイッチ オーバーレイを表示します。

スイッチインターフェイスには、ステータス表示もあります。スイッチインターフェイスは、スイッチに接続されているリンクの端にある小さな円としてレンダリングされます。スイッチインターフェイスを選択すると、カウンタテーブルの1つにデータが入力されます。マップには最新の接続が表示されます（タイム スライダーの設定には影響されません）。

ステップ 6 選択したフローおよびスイッチ インターフェイスのカウンタ データを表示します。

Switch Interface テーブルのデータは、パフォーマンス モニタリング（Performance Monitoring）および低速ドレイン（Slow Drain）から取り込まれます。ファブリックの [パフォーマンス モニタリング（Performance Monitoring）] を有効にして、低速ドレイン ジョブをスケジュールする必要があります。この表は **NA** を示し、それ以外の場合

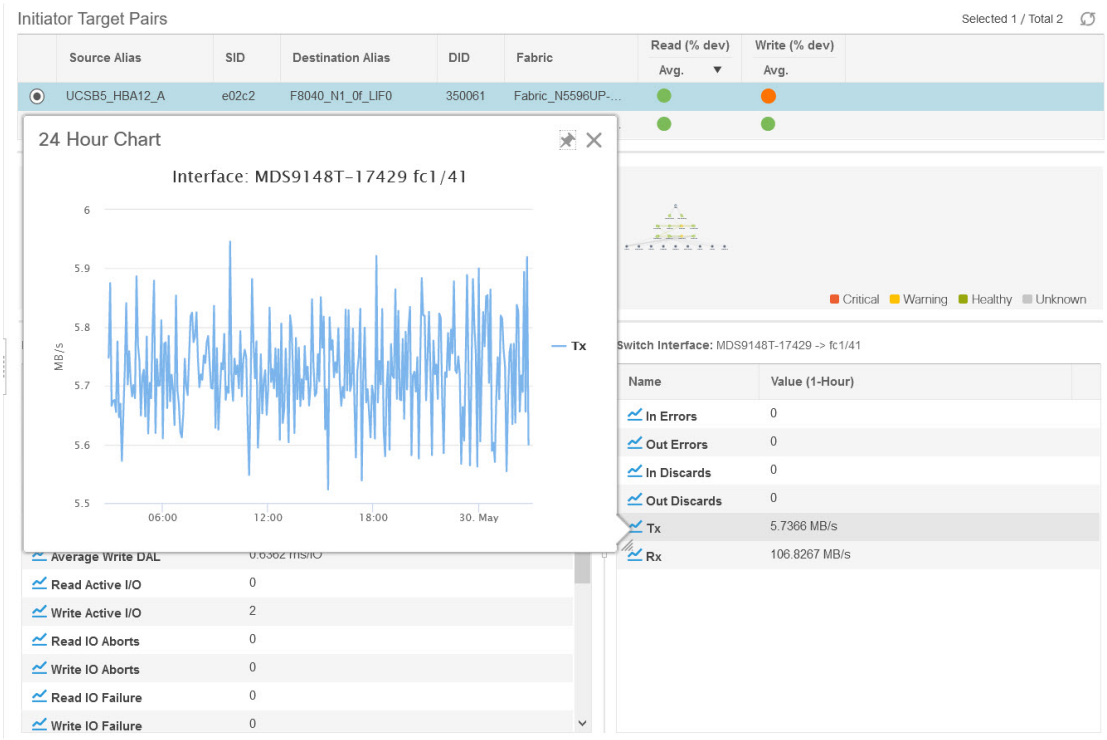
[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [SAN コレクション（SAN Collections）] を選択してパフォーマンス コレクションを有効にします。モニタするファブリックを選択します。ファブリックに対するすべてのパラメータ チェック ボックスをオンにします。**[適用（Apply）]** クリックして、パフォーマンスのモニタを開始します。

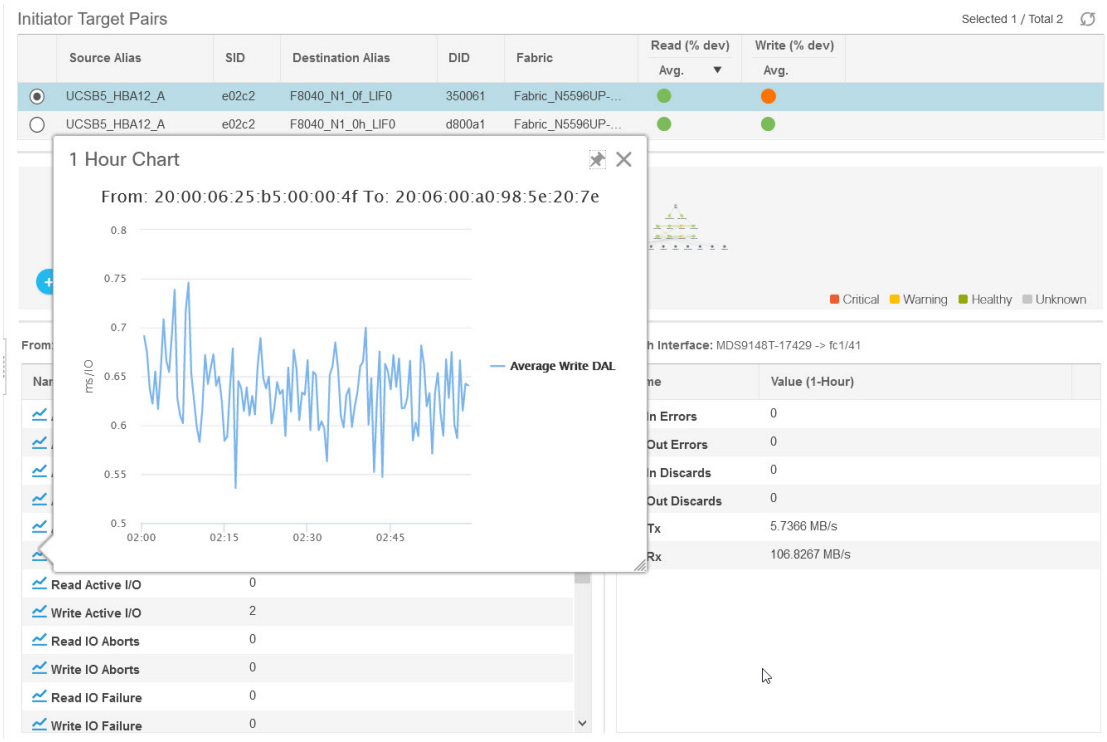
低速ドレイン メトリックを有効にするには、**[モニタ（Monitor）] > [SAN] > [低速ドレイン（Slow Drain Analysis）]** を選択します。ファブリックで現在のジョブを構成します。**[SAN Insights のモニタリング（Monitoring SAN Insights）]** で、マップ上のインターフェースをクリックします。**低速ドレイン メトリクス**は、スイッチ インターフェイス テーブルに表示されます。

- IT フローを選択して、左下の表にスイッチ テレメトリ インフラストラクチャからのトポロジとフロー メトリックを表示します。

  トポロジ ビューで特定のインターフェイスを選択して、ポートモニタリングインフラストラクチャからのインターフェイス メトリックを表示します。リリース 11.4(1) 以降、選択したエンクロージャ/IT ペアに対応するインターフェイスがデフォルトで選択されます。

ステップ 7 フローテーブルとスイッチインターフェイステーブルで、  アイコンをクリックして 24 時間チャートを表示します。


Initiator Target Pairs
Selected 1 / Total 2
Source Alias
SID
Destination Alias
DID
Fabric
Read (% dev)
Avg.
Write (% dev)
Avg.
UCSB5_HBA12_A
e02c2
F8040_N1_0f_LIF0
350061
Fabric_N5596UP-...
24 Hour Chart
Interface: MDS9148T-17429 fc1/41
MB/s
Tx
06:00
12:00
18:00
30. May
Critical
Warning
Healthy
Unknown
Switch Interface: MDS9148T-17429 -> fc1/41
Name
Value (1-Hour)
In Errors
Out Errors
In Discards
Out Discards
Tx
5.7366 MB/s
Rx
106.8267 MB/s
Read Active I/O
Write Active I/O
Read IO Aborts
Write IO Aborts
Read IO Failure
Write IO Failure

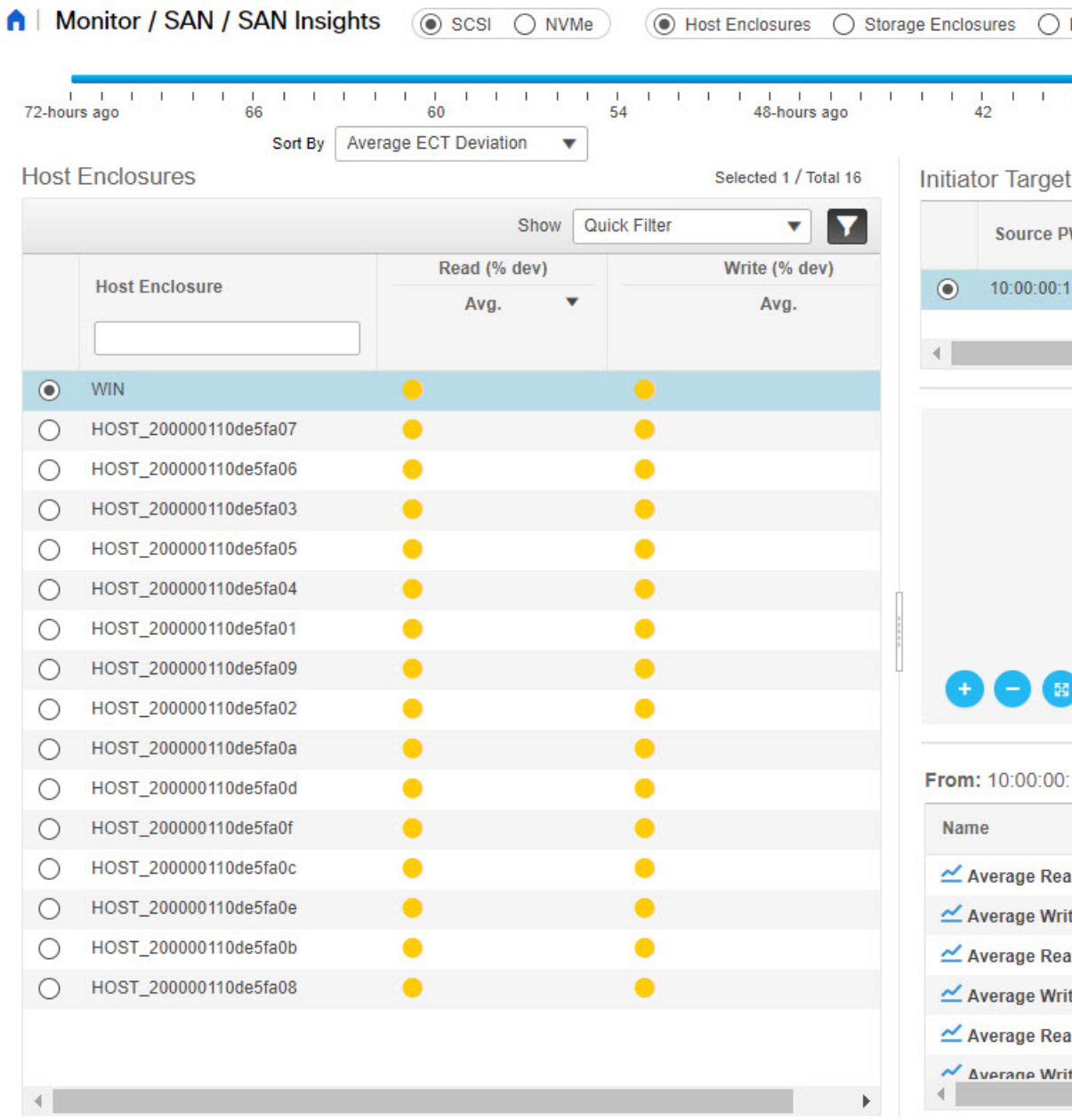

Initiator Target Pairs
Selected 1 / Total 2
Source Alias
SID
Destination Alias
DID
Fabric
Read (% dev)
Avg.
Write (% dev)
Avg.
UCSB5_HBA12_A
e02c2
F8040_N1_0f_LIF0
350061
Fabric_N5596UP-...
UCSB5_HBA12_A
e02c2
F8040_N1_0h_LIF0
d800a1
Fabric_N5596UP-...
1 Hour Chart
From: 20:00:06:25:b5:00:00:4f To: 20:06:00:a0:98:5e:20:7e
ms/IO
Average Write DAL
02:00
02:15
02:30
02:45
Critical
Warning
Healthy
Unknown
Value (1-Hour)
In Errors
Out Errors
In Discards
Out Discards
Tx
5.7366 MB/s
Rx
106.8267 MB/s
Read Active I/O
Write Active I/O
Read IO Aborts
Write IO Aborts
Read IO Failure
Write IO Failure

ホスト ラックの表示

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

Cisco DCNM 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：

1. **[モニター（Monitor）] > [SAN] > [San インサイト（SAN Insights）]** を選択し、**[ホスト エンクロージャ（Host Enclosure）]** を選択します。



2. タイム スライダーを使用して時間間隔を指定します。
3. すべてのホスト エンクロージャが一覧表示されている **[ホスト エンクロージャ（Host Enclosures）]** テーブルからホストを選択します。
4. イニシエータ ターゲット ペア テーブルから**[イニシエータとターゲットのペア（Initiator Target Pairs）]**を 1 つ選択します。

   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。

5. トポロジ マップからスイッチ インターフェイスを選択します。

   リリース 11.4(1) から、スイッチ インターフェイスがデフォルトで選択されます。**[スイッチ インターフェイス（Switch Interface）]**：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（for the last hour period selected）]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。

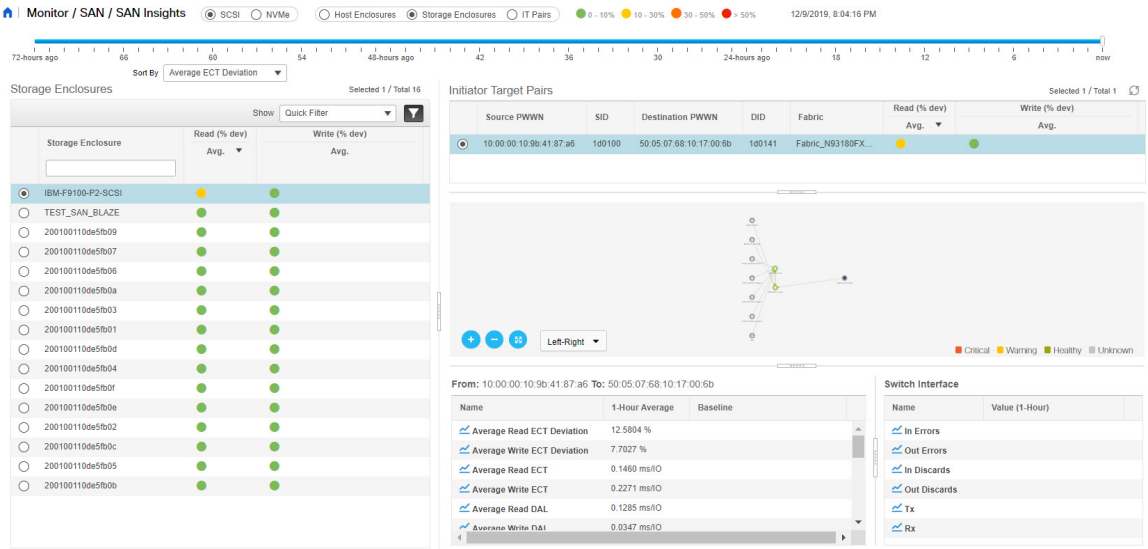
6. **[イニシエータ ターゲット ペア（Initiator Target Pairs）]** テーブルの **[読み取り (% dev)（Read (% dev)）]** または **[書き込み (% dev)（Write (% dev)）]** 列 にあるステータスの丸アイコンをクリックして、対応するイニシエータと事前にフィルタされたターゲット WWPN がある ECT 分析ウィンドウに移動します。

ストレージ エンクロージャの表示

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

Cisco DCNM 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。

1. **[モニタ（Storage Enclosures）] > [SAN] > [SAN Insights]** を選択し、**[ストレージ エンクロージャ（Storage Enclosure）]** を選択します。



2. タイム スライダーを使用して時間間隔を指定します。

3. **[ストレージ エンクロージャ（Storage Enclosures）]** テーブルからストレージ エンクロージャを選択します。
4. **[イニシエータ ターゲット ペア（Initiator Target Pairs）]** テーブルからイニシエータとターゲットのペアを選択します。
5. **[イニシエータ ターゲット ペア（Initiator Target Pairs）]** テーブルの **[読み取り (% dev)（Read (% dev)）]** または **[書き込み (% dev)（Write (% dev)）]** 列 にあるステータスの丸アイコンをクリックして、対応するイニシエータと事前にフィルタされたターゲットWWPNがある ECT 分析ウィンドウに移動します。
6. 選択したイニシエータとターゲットのペアおよびフロー メトリックを表すトポロジ マップを表示します。

   フロー メトリクスがフロー テーブルに表示されます。
7. トポロジ マップからスイッチ インターフェイスを選択します。

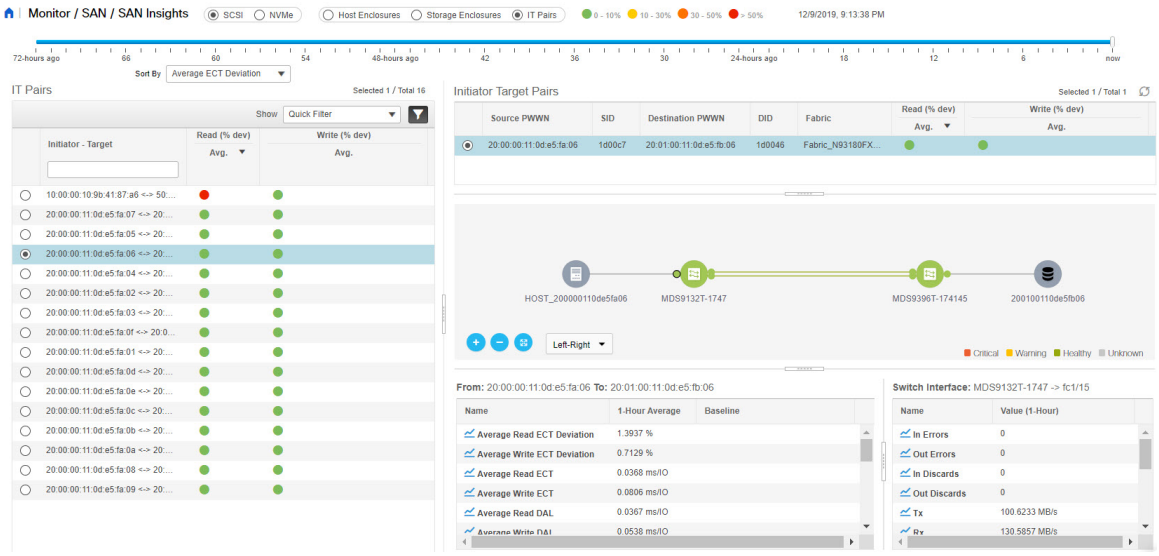
   [スイッチ インターフェイス（Switch Interface）] テーブルには、選択されたインターフェイスのデータが表示されます。リリース 11.4(1) から、スイッチ インターフェイスがピックアップされ、デフォルトで選択されます。

IT ペア の表示

リリース 11.3(1) から Cisco DCNM 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、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** 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。(Linux で SanInsight サービスを再起動するか、SAN-OVA/ISO/SE 展開でポスト プロセッサ アプリを一時停止/再開します)

Cisco DCNM Web UI から IT ペアを表示するには、次の手順を実行します。

1. **[モニタ（Monitor）] > [SAN] > [SAN Insights]** を選択してから、> **[IT Pairs（IT ペア）]** を選択します。



2. タイム スライダーを使用して時間間隔を指定します。
3. **[IT ペア（IT Pairs）]** テーブルからフローを選択します。

   イニシエータとターゲットのペアが **[イニシエータ ターゲット ペア]** テーブルに一覧表示され、選択した IT ペアのトポロジマップが表示されます。フローメトリックは、[IT ペア] テーブルに表示されます。
4. このウィンドウのフロー テーブルには、ECT/DAL/読み取り/書き込み時間、アクティブな I/O、中止、失敗などに関するすべてのメトリックに関する詳細が表示されます。

   また、フロー テーブルには 1 時間の平均とベースライン情報が表示されます。
5. **イニシエータ ターゲット ペア** テーブルのステータス ボールをクリックします。

   選択した IT ペアの 24 時間正規化 R/W ECT 偏差グラフが表示されます。
6. トポロジ マップからスイッチ インターフェイスを選択します。

   [スイッチ インターフェイス（Switch Interface）] テーブルには、選択されたインターフェイスのデータが表示されます。

LAN のモニタリング

LAN メニューには次のサブメニューが含まれます。

イーサネットに関するパフォーマンス情報のモニタリング

Cisco DCNM Web UI からイーサネットのパフォーマンス情報を監視するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [ローカル エリア ネットワーク（LAN）] > [イーサネット（Ethernet）]** を選択します。

[イーサネット（Ethernet）] ウィンドウが表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタできます。

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、次の手順を実行することもできます。

- **[名前（Name）]**カラムからイーサネット ポート名を選択すると、過去24時間にそのイーサネット ポートを通過したトラフィックを示すグラフが表示されます。時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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。
- 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 **[データの補間はしないでください（Do not interpolate data）]**することもできます。

  Note **[データの補間はしないでください（Do not interpolate data）]** オプションを使用するために**[サーバー プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- Rx/Tx の計算については、以下の Rx/Tx 計算を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、しきい値セクションを参照してください。

Note トラフィックの表示単位をバイトからビットに変更するには、Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**pm.showTrafficUnitAsbit** プロパティに true として値を入力し、**[変更を適用（Apply Changes）]** をクリックします。

ISL トラフィックとエラーのモニタリング

Cisco DCNM Web UI から ISL トラフィックとエラーをモニタするには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [LAN] > [リンク（Link）]** を選択します。

[ISL トラフィックとエラー（ISL Traffic and Errors）] ウィンドウが表示されます。このパネルには、その範囲内のエンドデバイスの ISL 情報が表示されます。範囲メニューを使用して、表示される範囲を縮小または拡大できます。

ステップ 2 ドロップダウンを使用して、の[過去 10 分、過去 1 時間、前日、先週、先月、および昨年（Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year）]で表示するようにフィルタ処理できます。

Note データ グリッドの **NaN**（非数）は、データが利用できないことを意味します。

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 ISL の詳細情報を表示することもできます。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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 **[データの補間はしない（Do not interpolate data）]**を設定することもできます。

  Note **[データの補間はしないでください（Do not interpolate data）]** オプションを使用するために**[サーバ プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- データをスプレッドシートにエクスポートするには、**[チャート（Chart）]** メニューのドロップダウン リストから **[エクスポート（Export）]** を選択し、**[保存（Save）]** をクリックします。
- Rx/Tx の計算については、以下の Rx/Tx 計算を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

Note パフォーマンステーブルにデータが含まれていない場合は、パフォーマンス設定のしきい値セクションを参照してパフォーマンスをオンにします。

vPC のモニタリング

仮想ポート チャネル（vPC）は、シングル ポート チャンネルとして違うデバイスに物理的に接続されたリンクを表示することをイネーブル化します。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロードバランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やす拡張された形式のポート チャンネルです。トラフィックは、2 つの単一デバイス vPC エンドポイント間で分散されます。vPC 構成に矛盾がある場合、vPC は正しく機能しません。

Note **[vPC パフォーマンス（vPC Performance）]**で vPC を表示するには、プライマリ デバイスとセカンダリ デバイスの両方をユーザーに指定する必要があります。いずれかのスイッチが指定されていない場合は、vPC 情報が再生されます。

Cisco DCNM **[Web クライアント（Web Client）] > [モニタ（Monitor）] > [vPC]** は、一貫性のある vPC のみを表示します。一貫性のある vPC と一貫性のない vPC の両方が表示されます。

Cisco DCNM **[Web UI] > [構成（Configure）] > [展開する（Deploy）] > [vPC ピア（vPC Peer）]** および **[Web クライアント（Web Client）] > [構成（Configure）] > [展開する（Deploy）] > [vPC]** を使用して、矛盾する vPC を特定し、各 vPC の矛盾を解決できます。

Table 10: vPC パフォーマンス, on page 140 は、データ グリッド ビューに次の vPC 構成の詳細を表示します。

***Table 10: vPC* パフォーマンス**

列	説明
検索ボックス	任意の文字列を入力して、それぞれの列のエントリをフィルタリングします。
vPC ID	vPC 識別子の構成済みデバイスを表示します。
ドメイン ID	vPC ピア スイッチのドメイン ID を表示します。
マルチ シャーシ vPC エンドポイント	vPC ドメインの下の各 vPC ID のマルチシャーシ vPC エンドポイントを表示します。
プライマリ vPC ピア - デバイス名	vPC プライマリ デバイス名を表示します。
プライマリ vPC ピア - プライマリ vPC インターフェイス	プライマリ vPC インターフェイスを表示します。
プライマリ vPC ピア - 容量	プライマリ vPC ピアの容量を表示します。

列	説明
プライマリ vPC ピア - 平均受信/秒	プライマリ vPC ピアの平均受信速度を表示します。
プライマリ vPC ピア - 平均送信/秒	プライマリ vPC ピアの平均送信速度を表示します。
プライマリ vPC ピア - ピーク使用率	プライマリ vPC ピアのピーク使用率を表示します。
セカンダリ vPC ピア - デバイス名	vPC セカンダリ デバイス名を表示します。
セカンダリ vPC インターフェイス	セカンダリ vPC インターフェイスを表示します。
セカンダリ vPC ピア - 容量	セカンダリ vPC ピアの容量を表示します。
セカンダリ vPC ピア - 平均。受信/秒	セカンダリ vPC ピアの平均受信速度を表示します。
セカンダリ vPC ピア - 平均。送信/秒	セカンダリ vPC ピアの平均送信速度を表示します。
セカンダリ vPC ピア - ピーク使用率	セカンダリ vPC ピアのピーク使用率を表示します。

この機能は次のように使用できます。

vPC パフォーマンスのモニタリング

一貫性のある仮想ポートチャネル(vPC)間の関係を表示できます。すべてのメンバーインターフェイスの統計と、ポート チャネル レベルでの統計の集約を表示できます。

Note このタブには、一貫性のある vPC のみが表示されます。

Cisco DCNM Web UI から VPC パフォーマンス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 **[モニタ（Monitor）] > [LAN] > [vPC]** を選択します。

vPC パフォーマンス統計が表示されます。すべての vPC の集約された統計が表形式で表示されます。

ステップ 2 **[vPC ID]** をクリックします。

vPC トポロジ、**vPC の詳細**、**ピア リンクの詳細**、および**ピア リンクのステータス**が表示されます。

vPC の **vPC 整合性**、**ピア リンク整合性**、および **vPC Type2 整合性**が表示されます。

- **[vPC の詳細]** タブをクリックすると、プライマリとセカンダリの両方の vPC デバイスの vPC **基本設定**と**レイヤ 2 設定**のパラメータの詳細を表示できます。

- **[ピア リンクの詳細]** タブをクリックして、プライマリとセカンダリの両方の vPC デバイスのピア リンク **vPC グローバル設定**および **STP グローバル設定**のパラメータの詳細を表示します。
- **[ピア リンクのステータス]** タブをクリックすると、**vPC の整合性** が表示され、**ピア リンクの整合性** ステータスが表示されます。プライマリとセカンダリの両方の vPC デバイスの**ロール ステータス**と **vPC ピア キープアライブ ステータス**のパラメータの詳細も表示されます。

ステップ 3 **[プライマリ vPC ピア]** または **[セカンダリ vPC ピア]** 列の**デバイス名**の前にあるピア リンク アイコンをクリックして、そのメンバー インターフェイスを表示します。

ステップ 4 対応するインターフェイスの **[チャートの表示（Show Chart）]** アイコンをクリックして、履歴統計を表示します。

トラフィック分散統計は、vPC ウィンドウの下部に表示されます。デフォルトでは、Cisco DCNM Web クライアントは 24 時間の履歴統計を表示します。

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フローの詳細情報を表示することもできます。

- 時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 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 **[データの補間はしない（Do not interpolate data）]** を設定することもできます。

  Note **[データの補間はしない（Do not interpolate data）]** オプションを使用するために **[サーバー プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- vPC Utilization データを印刷するには、右上隅にある **[印刷（Print）]** アイコンをクリックします。[vPC 使用率（vPC Utilization）] ページが表示されます。
- 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。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、しきい値セクションを参照してください。

モニタリング レポート

レポート メニューには次のサブメニューが含まれます。

レポートの表示

次の選択オプションに基づいて保存されたレポートを表示できます。

- **By Template**
- **By User**
- メニュー バーから、**[モニタ（Monitor）] > [レポート（Report）] > [表示（View）]** を選択します。

Cisco DCNM Web UI からレポートを表示するには、次の手順を実行します。

Procedure

ステップ 1 左側のペインで、**By Template**もしくは、**By User**フォルダを展開します。

ステップ 2 表示するレポートを選択します。

レポートをメイン スクリーンで表示するもしくは、 **Report**カラムでレポートを選択し HTML バージョンのレポートを新しいブラウザで表示することができます。

ステップ 3 特定のレポートを削除するには、チェック ボックスを選択し**[削除（Delete）]**アイコンをクリックします。

ステップ 4 すべてのレポートを削除するには、ヘッダーのチェック ボックスをチェックして**[削除（Delete）]** アイコンをクリックします。

Note 複数のファブリックがある場合、範囲で DCNM-SAN グループを選択して、単一のレポートで複数のファブリックのホストからストレージへの接続を表示できます。

レポートは 2 つのセクションに分かれています。

- 障害のあるモジュールがあるすべてのデバイスの概要レポート。表示には、デバイスのホスト名、障害のあるモジュールの数、およびモジュール番号とその PID を含む、すべてのデバイスの情報が表示されています。
- モジュールのデバイスに関する情報。この表には、失敗したテストに関する詳細が含まれています。

フェデレーション設定でのレポート ジョブのスケジューリング

フェデレーションのさまざまなサーバでレポート ジョブをスケジュールするには、Cisco DCNM Web UI で、次の手順を実行します。

1. Server1 で事前定義またはユーザー定義のレポート ジョブをスケジュールします。

   [モニタ（Monitor）] > [レポート（Report）] > [生成（Generate）] を選択します。詳細な手順については、レポートの生成, on page 144 を参照してください。

2. **[モニタ（Monitor）] > [レポート（Report）] > [ジョブ（Jobs）]** を選択し、ジョブが正しくスケジュールされていることを確認します。
3. Server2 で事前定義またはユーザー定義のレポート ジョブをスケジュールします。

Note フェデレーション セットアップで第 1 サーバ、第 2 サーバ、第 3 サーバを順番に構成するようにします。

レポートの生成

選択したテンプレートに基づいてレポートを生成したり、指定時間に実行するようにレポートのスケジュールを作成できます。

Procedure

ステップ 1 メニュー バーから、**[モニタ（Monitor）] > [レポート（Report）] > [生成（Generate）]** を選択します。

[レポートの生成（Generate Report）] ウィンドウが表示されます。

ステップ 2 設定画面で、ドロップダウンを使用してレポート生成の範囲を定義します。

[範囲（Scope）] ドロップダウンで、デュアル ファブリックを持つ範囲グループを選択できます。ホストとストレージ エンド デバイスによって生成されたトラフィック データが並べて表示されるため、デュアル ファブリックで生成されたトラフィック データを表示および比較できます。このレポートを表示するには、**[その他の事前定義（Other Predefined）]** フォルダで、**[VSAN ごとのトラフィック（デュアル ファブリック（Traffic by VSAN (Dual Fabrics)）]** を選択します。[オプション（Options）] をクリックして、**デバイス タイプ**と**ファブリック**を選択します。[保存（Save）] をクリックして、設定を保存します。

ステップ 3 左側のペインでフォルダーを展開し、レポートを選択します。

ステップ 4 （オプション）右側のペインで、**[レポート名（Report Name）]**を編集できます。

ステップ 5 （オプション）**[Csv/Excel にエクスポート（Export to Csv/Excel）]** チェックボックスを選択し、レポートを Microsoft Excel スプレッドシートにエクスポートします。

ステップ 6 **[繰り返し（Repeat）]** ラジオ ボタンで、次を選択した場合：

- **[なし（Never）]** - レポートは現在のセッション中にのみ生成されます。
- **[1 回（Once）]** - レポートは、現在のセッションとは別に、指定された日時に生成されます。
- **[毎日（Daily）]** - 指定した時間の開始日と終了日に基づき、レポートが毎日生成されます。

- **[毎週（Weekly）]** - 指定した時間で開始日および終了日に基づき 1 週間に 1 回レポートが生成されます。
- **[毎月（Monthly）]** - 指定した時間の開始日と終了日に基づき、レポートが 1 ヶ月に 1 回生成されます。

ネットワーク構成監査のレポートを生成すると、日次ジョブは、選択したデバイスの過去1日間のレポートを生成します。同様に、週次ジョブは過去7日間のレポートを生成し、月次ジョブは過去 30 日間のレポートを生成します。

ステップ 7 **[作成（Create）]** ボタンをクリックして、仕様に基づいたレポートを生成します。

新しいブラウザ ウィンドウにレポートの結果が表示されます。

または、**[モニタ（Monitor）] > [レポート（Report）] > [表示（View）]** を選択し、ナビゲーション ウィンドウで使用するレポート テンプレートからレポート名を選択し、レポートを表示できます。

Note **開始日**には**終了日**より 5 分以上前の時刻を指定します。

レポートは 2 つのセクションに分かれています。

- 障害のあるモジュールがあるすべてのデバイスの概要レポート。テーブルには、デバイスのホスト名、障害のあるモジュールの数、およびモジュール番号とその PID を含む、すべてのデバイスの情報が表示されます。
- モジュールのデバイスの詳細情報。この表には、失敗したテストに関する詳細が含まれています。

SAN ユーザー定義レポートの作成

Cisco DCNM-SAN によって取得される情報のすべてまたは任意のサブセットからカスタム レポートを作成できます。レポートに取り込みたいイベント、パフォーマンス、およびインベントリの統計情報を選択することによってレポートを作成し、対象とする SAN、ファブリック、または VSAN を設定してテンプレートの範囲を制限します。このテンプレートに基づいて、すぐにまたはあとで、ファブリックのレポートの生成や、スケジュール作成を実行できます。Cisco DCNM Web クライアントは、レポート テンプレートとレポート作成時間に基づいて生成される各レポートを保存します。

Cisco MDS NX-OS リリース 5.0 以降、以前のバージョンの制限を解消するためにレポート テンプレート設計が変更されました。新しい設計モデルでは、単一ページで追加機能、削除機能、および変更機能を実行できます。新しいナビゲーション システムでは複数のファブリックや VSAN を選択でき、将来的に新しい品目やカテゴリを追加するための拡張性に優れています。

新しい設計モデルには、次の 3 つのパネルがあります。

- **[テンプレート（Template）]** パネル：**[テンプレート（Template）]** パネルでは、新規テンプレートの追加、既存テンプレートの変更、および既存テンプレートの削除を行えます。

- **[構成（Configuration）]** パネル：**[構成（Configuration）]** パネルでは、新規テンプレートを追加するときに構成したり、既存テンプレートを変更したりすることができます。[Configuration] パネル内のオプションは、新規テンプレートを追加するか、既存テンプレートを選択するまでディセーブルになります。[Configuration] パネルの上部には、選択して設定できる多数のカテゴリがあります。
- **[ユーザー選択（User Selection）]** パネル - **[ユーザー選択（User Selection）]** パネルは、リアルタイムで構成オプションを表示します。[構成（Configuration）] パネルには一度に 1 つのカテゴリに関する情報しか表示できませんが、**[ユーザー選択（User Selection）]** パネルにはすべての選択または設定を表示できます。

Cisco DCNM Web UI からレポートを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）]** > **[レポート（Report）]** > **[ユーザー定義（User Defined）]** を選択します。

[ユーザー定義の作成（Create User-Defined）] ウィンドウが表示されます。

ステップ 2 **[テンプレート（Template）]** パネルの **[名前（Name）]** 列で、**[クリックして新しいカスタムを追加（CLICK TO ADD NEW CUSTOM）]** を選択して、新しいレポートの**名前**を編集します。

ステップ 3 **[構成（Configuration）]** パネルの **[範囲（Scope）]** をクリックして、レポートの範囲を定義します。デフォルトの範囲には、データセンター、SAN、LAN、およびファブリック構成が含まれます。

ステップ 4 **[インベントリ（Inventory）]** をクリックし、チェックボックスを使用して、レポートに必要なインベントリ情報を選択します。また、ドロップダウンを使用して、レポートに必要な上位のパフォーマンスとタイムラインを選択することでフィルタリングすることもできます。

ステップ 5 **[パフォーマンス（Performance）]** をクリックし、チェックボックスを使用して、レポートに必要なパフォーマンス情報を選択します。

ステップ 6 **[ヘルス（Health）]** をクリックし、チェックボックスを使用して、レポートに必要なヘルス情報を選択します。

ステップ 7 **[保存（Save）]** をクリックして、このレポート テンプレートを保存します。

レポートが保存されたことを確認する確認メッセージが表示されます。

レポートテンプレートを消去

Cisco DCNM ウェブ UI からレポート テンプレートを削除するには、以下の手順を実行します。

Procedure

ステップ 1 **[Template（テンプレート）]** パネルで、削除するレポート テンプレートを選択します。

ステップ 2 レポートを削除するには、**[削除（Delete）]** アイコンをクリックします。

ステップ 3 確認ポップアップで、**[はい（Yes）]** をクリックしてテンプレートを削除します。

カスタム レポート テンプレートの修正

Procedure

ステップ 1 **[モニタ > レポート > ユーザ定義（Monitor > Report > User Defined）]**を選択します 。

[テンプレート（Template）]、**[構成（Configuration）]**、および**[ユーザ選択（User Selection）]** の各パネルが表示されます。

ステップ 2 **[テンプレート（Template）]** パネルからレポートを選択します。

このレポートの現在の情報が **[ユーザ選択（User Selection）]** パネルに表示されます。

ステップ 3 **[構成（Configuration）]**パネルで情報を変更します。

ステップ 4 **[保存（Save）]** をクリックして、レポート テンプレートを保存します。

レポートが保存されていることを確認メッセージが表示されることで確認します。

Note 既存のレポートの範囲を変更することはできません。新しい範囲の新しいレポートを生成します。

レポート テンプレートに基づくスケジュール済みのジョブを表示

レポート テンプレートに基づくスケジュール済みジョブを Cisco DCNM Web UI から表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [レポート（Report）] > [ジョブ（Jobs）]** を選択します。

[レポート ジョブ（Report Jobs）] ウィンドウは、生成のスケジュール済みのレポートの詳細とステータスを表示します。

ステップ 2 特定のレポートのチェックボックスを選択し、**[削除（Delete）]**アイコンをクリックしてレポートを削除します。

アラーム

アラーム メニューには次のサブメニューが含まれます。

アラームとイベントの表示

アラーム、クリアされたアラーム、およびイベントを表示できます。

Procedure

ステップ 1 **[モニタ（Monitor）] > [アラーム（Alarms）] > [表示（View）]** を選択します。

ステップ 2 次のいずれかのタブを選択します。

- **[Alarms（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。
- **[クリアされたアラーム（Cleared Alarms）]**：このタブには、クリア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、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。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。
- **[Events（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**、**確認済みユーザー**、**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。

アラーム ポリシーの監視と追加

Note

- アラームポリシーは、計算ノードに保存されます。したがって、DCNM のバックアップを取得することに加えて、各計算ノードで **appmgr backup** コマンドを実行します。

Windows および Linux での Cisco DCNM SAN フェデレーション展開では、プライマリ ノードとセカンダリ ノードの両方で、サーバ プロパティの **alarm.enable.external** 値が true に設定されていることを確認します。**[管理 (Administration)] > [DCNM サーバー (DCNM Server)] > [サーバー ステータス (Server Status)]** を選択します。**alarm.enable.external** フィールドを見つけて、**true** に設定されていることを確認します。これを有効にするには、DCNM サーバーを再起動する必要があります。

アラームを DCNM の登録済み SNMP リスナーに転送できます。Cisco DCNM Web UI から、**[Administration（管理）] > [DCNM Server（DCNM サーバー）] > [Server Properties（サーバーのプロパティ）]** 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、**[Apply Changes（変更の適用）]** をクリックして、DCNM サービスを再起動します。

Note **[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。

次のアラーム ポリシーを追加できます。

- **デバイスの正常性**：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。
- **インターフェイス正常性ポリシー**：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**：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。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [アラームポリシー（Alarm Policies）]** を選択します。

ステップ 2 **[アラームを有効にする]** チェック ボックスをオンにして、アラーム ポリシーを有効にします。

ステップ 3 **[追加（Add）]** ドロップダウンリストから、次のいずれかのログイン情報を選択します。

- デバイス正常性ポリシー：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。詳細なトラップ OID 定義については、https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en を参照してください。
- インターフェイス正常性ポリシー：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、リンクステート、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、インバウンド廃棄、およびアウトバウンド廃棄を指定します。

- Syslogアラーム ポリシー：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。
  - 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。シンタックスは次のとおりです。**Facility-Severity-Type: Message**
  - Clear Regex：syslog クリア メッセージの形式を定義します。シンタックスは次のとおりです。**Facility-Severity-Type: Message**

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。

Table 11:* 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。

識別子	ID1-ID2
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。

Table 12: 例 2

識別子	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

Table 13: 例 3

識別子	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

ステップ 4 **[OK]**をクリックしてポリシーを追加します。

端末モニターとコンソールの syslog メッセージ

次の例は、syslog メッセージが端末モニタとコンソールにどのように表示されるかを示しています。正規表現は、syslog メッセージの % 記号の後の部分と一致します。

```
leaf-9516# terminal monitor
leaf-9516# conf t
leaf-9516(config)# int e15/1-32
leaf-9516(config-if-range)# no shut
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/1 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/1 is down (Transceiver Absent)
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/2 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/2 is down (Transceiver Absent)
2019 Aug 2 04:41:28 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/3 is admin up .
```

コンソールの syslog メッセージは、%$ 記号で囲まれた追加のポート情報を除いて、端末モニタに表示されるものと同様の形式です。ただし、正規表現は、syslog メッセージの最後の % 記号の後の部分と一致します。

```
SR-leaf1# 2019 Aug 26 23:55:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-
PFM_ALERT: FAN_BAD: fan6
2019 Aug 26 23:56:15 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:18 SR-leaf1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL:
System ready
2019 Aug 26 23:56:25 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:35 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED:
The guest shell has been enabled. The command 'guestshell' may be used
to access it, 'guestshell destroy' to remove it.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FAN_REMOVED: Fan
module 5 (Serial number ) Fan5(sys_fan5) removed
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 2 minutes 0 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 1 minutes 40 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK:
Fan module 5 (Fan5(sys_fan5) fan) ok
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

アクティブなポリシー

新しいアラーム ポリシーを作成したら、それらをアクティブにします。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarm Policies）]**を選択します。

ステップ 2 アクティブ化するポリシーを選択し、**[アクティブ化]** ボタンをクリックします。

ポリシーの非アクティブ化

アクティブなアラーム ポリシーを非アクティブ化できます。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。
ステップ 2 非アクティブ化するポリシーを選択し、**[非アクティブ化]** ボタンをクリックします。

ポリシーのインポート

インポート機能を使用してアラーム ポリシーを作成できます。

Procedure

ステップ 1 **[モニター] > [アラーム] > [ポリシー]** を選択し、**[インポート]** ボタンをクリックします。
ステップ 2 コンピュータに保存されているポリシー ファイルを参照して選択します。

ポリシーはテキスト形式でのみインポートできます。

ポリシーのエクスポート

アラーム ポリシーをテキスト ファイルにエクスポートできます。

Procedure

ステップ 1 メニュー バーから **[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]** を選択します。
ステップ 2 **[エクスポート]**ボタンをクリックし、エクスポートしたファイルを保存するコンピューター上の場所を選択します。

ポリシーの編集

Procedure

ステップ 1 メニュー バーから**[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。
ステップ 2 編集するポリシーを選択します。
ステップ 3 **[編集（Edit）]** ボタンをクリックして変更を加えます。
ステップ 4 [OK] ボタンをクリックします。

ポリシーの削除

Procedure

ステップ 1 メニュー バーから**[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。

ステップ 2 削除するポリシーを選択します。

ステップ 3 **[削除（Delete）]** ボタンをクリックします。ポリシーが削除されます。

外部アラームの有効化

次のいずれかの方法を使用して、外部アラームを有効にできます。

- Cisco DCNM Web UI を使用します。
  1. **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** Cisco DCNM Web UI を選択します。
  2. **alarm.enable.external** プロパティを見つけます。
  3. フィールドに値として **true** を入力します。
- REST API の使用
  1. DCNM セットアップから API ドキュメントの URL に移動します: https://<*DCNM-ip*>/api-docs
  2. **[アラーム（Alarms）]** セクションに移動します。
  3. **[POST] > [rest/alarms/enabledisableextalarm]** をクリックします。
  4. **[値（Value）]** ドロップダウン リストから、**[body（本体）]** パラメータ値として **[true]** を選択します。
  5. **[試してみる!（Try it out!）]** をクリックします。
- CLI の使用
  1. SSH を使用してDCNM サーバにログインします。
  2. server.properties ファイルで、**alarm.enable.external** プロパティを **true** に設定します。

     ファイルパスは `/usr/local/cisco/dcm/fm/config/server.properties` です。

ヘルス モニタ アラーム

Cisco DCNM リリース 11.4(1) 以降、アラームはヘルス モニタ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。

ヘルス モニタ：アラーム ポリシー

ヘルス モニタの外部アラーム カテゴリ ポリシーは、ファブリック内のすべてのデバイスで自動的にアクティブ化および有効化されます。このアラーム ポリシーの重大度は、マイナー、メジャー、または重大です。

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。

- Elasticsearch （ES）クラスタのステータスが赤：重大（クラスタ/HA モードの場合のみ）
- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 90%

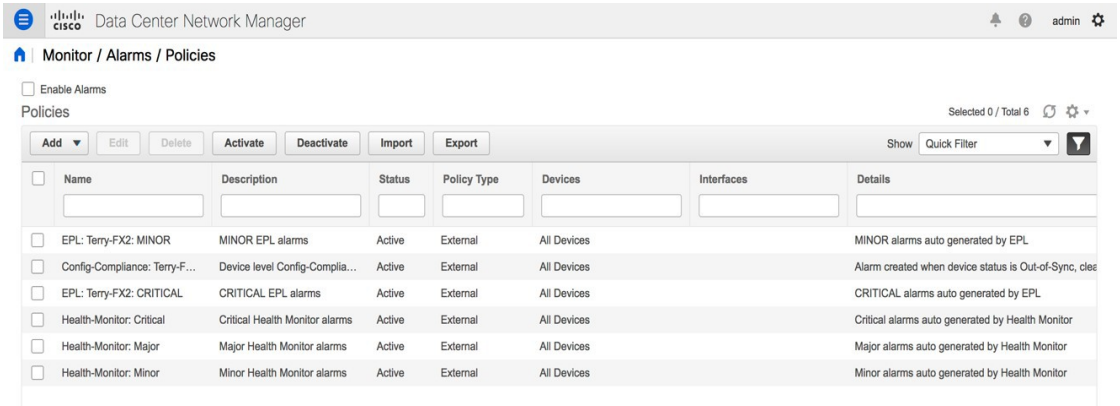
次のイベントの場合、アラームが発生し、メジャーとして分類されます。

- ES クラスタ ステータスが黄色（クラスタ/HA モードの場合のみ）
- ES に未割り当てのシャードがある（クラスタ/HA モードのみ）
- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 80% および <90%

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。

- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 65% および <80%
- Kafka: アクティブなリーダーのないパーティションの数 > 0
- Kafka: 適格なパーティション リーダーが見つかりません。不明確なリーダー > 0

[モニタ（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）] を選択して、ヘルス モニタのアラーム 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。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、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。



GUIを使用してアラームポリシーが非アクティブ化された場合、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、**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** 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、GUI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。

ヘルス モニタ：アクティブ アラーム

[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）] 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、**[ステータスを変更（Change Status）]**をクリックして **[クリア（Clear）]** を選択します。

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、**[削除（Delete）]** をクリックします。

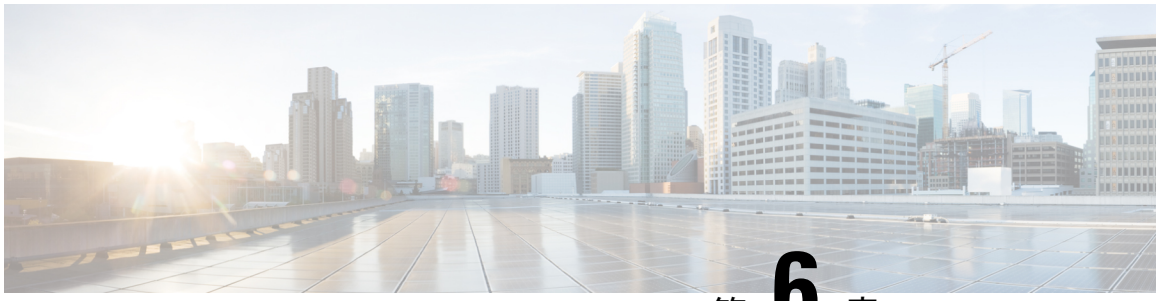
ヘルス モニタ：クリアされたアラーム

クリアされたアラームを表示するには **[モニタ（Monitor）]>[アラーム（Alarms）]>[表示（View）]>[クリアされたアラーム（Cleared Alarms）]**を選択します。

必須のアラームの詳細な情報を表示するには矢印アイコン ▶ をクリックします。

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、**[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、アラームを参照してください。



第 6 章

設定

この章は次のトピックで構成されています。

テンプレート （Templates）

[テンプレート（Templates）] メニューは、次のオプションが含まれます。

[テンプレート ライブラリ（Template Library）]

[テンプレート ライブラリ（Template Library）]には、次のタブが含まれています：

[テンプレート ライブラリ（Template Library）]

Cisco DCNM Web クライアントを使用して、異なる Cisco Nexus 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 DCNM Web クライアントのホームページから、**[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。Cisco DCNM Web クライアントで構成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。

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。

Table 14: テンプレート操作

フィールド	説明
Add Template	新しいテンプレートを追加できます。

フィールド	説明
ジョブ作成ウィザードの起動	ジョブを作成できます。
テンプレートの変更/表示	テンプレート定義を表示し、必要に応じて変更できます。
テンプレートに名前を付けて保存	選択したテンプレートを別の名前で保存できます。必要に応じて、テンプレートを編集できます。
テンプレートの削除（Delete Template）	テンプレートの削除を許可します
テンプレートのインポート	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。
テンプレートのエクスポート	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。
テンプレート Zip ファイルのインポート	`.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。

Note サーバーの再起動後にテンプレートのロード中に問題が発生した場合は、**[テンプレート Zip ファイルのインポート]** の横に通知が表示されます。通知をクリックして、**[テンプレートの読み込み中の問題]** ウィンドウにエラーを表示します。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。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。

Table 15: テンプレートのプロパティ

フィールド	説明
テンプレート名（Template Name）	構成されたテンプレートの名前が表示されます。
[テンプレートの説明（Template Description）]	テンプレートの構成中に提供される説明を表示します。
タグ（Tags）	テンプレートに割り当てられたタグを表示し、タグに基づいてテンプレートをフィルタリングするのに役立ちます。

フィールド	説明
対応プラットフォーム	テンプレートと互換性のあるサポートされている Cisco Nexus プラットフォームを表示します。テンプレートでサポートされているプラットフォームのチェック ボックスをオンにします。 **Note** 複数のプラットフォームを選択できます。
テンプレートのタイプ	テンプレートのタイプが表示されます。
テンプレート サブ タイプ	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。
テンプレートのコンテンツ タイプ	Jython または Template CLI のどちらであるかを指定します。

Table 16: 詳細テンプレートのプロパティ

フィールド	説明
実装	実装する抽象テンプレートを表示します。
依存関係	スイッチの特定の機能を指定します。
作成日：	テンプレートを公開するかどうかを指定します。
インポート	インポートのベース テンプレートを指定します。

さらに、メニュー バーから **[構成] > [テンプレート] > [テンプレート ライブラリ] > [テンプレート]** を選択し、次のこともできます。

- **[フィルタを表示]** をクリックして、ヘッダーに基づいたテンプレートをフィルタ処理します。
- **[印刷]** をクリックして、テンプレートのリストを印刷します。
- **[Excel にエクスポート]** をクリックして、テンプレートのリストを Microsoft Excel スプレッドシートにエクスポートします。

この項の内容は、次のとおりです。

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
templateType	使用するテンプレートのタイプを指定します。	• CLI • POAP • ポリシー • SHOW • プロファイル • ファブリック • [抽象（ABSTRACT）]	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 • ポリシー • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • interface-vlan • INTERFACE_VPC	

プロパティ名	説明	有効な値	任意かどうか
		• INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SUBPORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • プロファイル • VXLAN • ファブリック • 該当なし	

プロパティ名	説明	有効な値	任意かどうか
		• [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_SAN_PORT_CHANNEL • 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
contentType		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI • 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 • [抽象（ABSTRACT）] • TEMPLATE_CLI • PYTHON	はい
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
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

変数の型	有効値	反復可能?

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
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

変数の型	有効値	反復可能?

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。

wwn （Cisco DCNM 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							
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							

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
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			
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] 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 shakeline { [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>; ..... } {structinst} [, <structinst2> [, <structinst3> []>];												
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。
- インタラクティブ コマンドの処理：インタラクティブ コマンドを処理するためのテンプレート コンテンツの一部として、プロンプトと応答を含めます。

```
Example:

##template variables
string srcFile;
string srcDir;
string password;
string vrf;
##

##template content
copy scp://root@10.127.117.65/$$srcFile$$ bootflash: vrf $$vrf$$ <prompt:'(yes/no)?',
response:'yes'> <prompt:'(y/n)?[n]',
response:'y'> <prompt:'password:',
response:'$$password$$'>
```

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]**

テンプレート コンテンツ エディタ

テンプレート コンテンツ エディタには、次の機能があります。

- 構文の強調表示: エディタは、Python スクリプトのさまざまなタイプのステートメント、キーワードなどの構文を強調表示します。
- オートコンプリート: 入力を開始すると、エディタはテンプレートのデータ型、注釈、またはメタプロパティを提案します。
- 行に移動: スクロールする代わりに、テンプレート コンテンツ エディタで正確な行に移動できます。Mac の場合は **Command-L**、Windows の場合は **Ctrl-L** を押し、ポップアップ ウィンドウに移動先の行番号を入力します。

  エディタで行数より大きい値を入力すると、エディタ ウィンドウの最後の行に移動します。

- テンプレートの検索と置換: Mac の場合は **Command-F**、Windows の場合は **Ctrl-F** を押し、**検索対象**フィールドに検索語を入力し、検索ウィンドウで検索のタイプを選択します。エディタで次の検索を実行できます。
  - **RegExp 検索**：エディタで正規表現検索を実行できます。
  - **CaseSensitive 検索** ：エディタで大文字と小文字を区別した検索を実行できます。
  - **単語全体の検索 : 単語全体の検索を実行して、エディタで正確な単語を見つけることができます。**たとえば、"play" という単語の通常の検索では、"display" などの単語の一部である結果が返されますが、単語全体の検索では、"play" という単語に完全に一致する場合にのみ結果が返されます。
  - **選択範囲で検索** : 選択したコンテンツで検索を実行できます。検索を絞り込みたいコンテンツを選択し、検索語を入力します。

  置換オプションを使用するには、検索ウィンドウで + アイコンを選択します。**[置換後の文字列（Replace with）]** フィールドに置換する単語を入力します。**[置換]** を選択すると、選択した単語を 1 回だけ置き換えることができます。選択した単語の出現箇所をすべて置換するには、**[すべて]** を選択します。
- コードの折りたたみ: エディタでコード ブロックを展開またはグループ化するには、行番号の横にある矢印をクリックします。
- その他の機能: エディタは、コード、閉じ括弧を自動的にインデントし、対応する括弧を強調表示します。

テンプレート エディタの設定

[テンプレート エディタの設定（Template Editor Settings）] をクリックすると、テンプレート エディタの次の機能を編集できます。

- **[テーマ（Theme）]** : ドロップダウン リストからエディタに必要なテーマを選択します。
- **KeyBinding** : エディタをカスタマイズするには、**KeyBinding** ドロップダウン リストからエディタ モードを選択します。 **Vim** と **Ace** モードがサポートされています。デフォルトは **Ace** です。
- **[フォント サイズ（Font Size）]** : エディタに必要なフォント サイズを選択します。

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。

- VXLAN および FabricPath のソリューション POAP テンプレート

  Cisco DCNM リリース 10.0(1) 以降、シスコは POAP 操作を支援する定義済みテンプレートのセットを提供します。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。

  POAP テンプレートをダウンロードしてインストールする方法については、『*[Cisco DCNM 設置ガイド、リリース 10.0(x)*』を参照してください。

テンプレートの追加

Cisco Web UI からユーザー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 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。

[テンプレート プロパティ（Template Properties）] ウィンドウに、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、およびタグが表示されます。

ステップ 2 **[追加（Add）]** をクリックして新しいテンプレートを追加します。

[テンプレートのプロパティ（Properties）] ウィンドウが表示されます。

ステップ 3 [テンプレート名、詳細、タグとサポートされているプラットフォームを指定。（Specify a template name, description, tags, and supported platforms for the new template.）]

ステップ 4 テンプレートの**[テンプレート タイプ（Template Type）]**を指定します。[アプリケーションの電源を入れたときにこのテンプレートを使用できるようにするには、**POAP** を選択します。（Select POAP to make this template available when you power on the application.）]

Note **POAP** が選択されていない場合、テンプレートは CLI テンプレートと見なされます。

ステップ 5 テンプレートの**[テンプレート サブ タイプ（Template Sub Type）]**と**[テンプレート コンテンツ タイプ（Template Content Type）]**を選択します。

ステップ 6 **[詳細（Advanced）]** タブをクリックして、**[実装（Advanced）]**、**[依存関係（Dependencies）]**、**[公開（Published）]**、**[インポート（Imports）]**などの他のプロパティを編集します。**[発行済み（Published）]** を選択して、テンプレートを読み取り専用にします。公開されたテンプレートは編集できません。

ステップ 7 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレート チェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。ベース テンプレートには、テンプレート プロパティ、テンプレート変数、およびテンプレート コンテンツが表示されます。他のテンプレートにこのテンプレートをインポートすることができます。そして、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。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。

Note 基本テンプレートは CLI テンプレートです。

ステップ 8 **[OK]** をクリックしてテンプレートのプロパティを保存するか、ウィンドウの右上隅にあるキャンセル アイコンをクリックして変更を元に戻します。

Note **[テンプレート プロパティ（Template Property）]** をクリックして、テンプレート プロパティを編集できます。

ステップ 9 **[テンプレート コンテンツ（Template Content）]** をクリックして、テンプレートの構文を編集します。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 10 **[テンプレート構文の検証]** をクリックして、テンプレート値を検証します。

エラーまたは警告メッセージが表示された場合は、[エラーおよび警告フィールドをクリックして（by clicking the error and warnings field）]、**検証テーブル（Validation Table）** で検証の詳細を確認できます。

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 11 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 12 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレート ジョブの構成

Cisco DCNM Web UI から単独テンプレートのジョブを構成と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 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。

ステップ 2 テンプレートを選択します。

Note Config Job ウィザードは、CLI テンプレートにのみ適用できます。

ステップ 3 **[ジョブ作成ウィザードの起動（Launch job creation wizard）]** アイコンをクリックし、**[次へ（Next）]** をクリックします。

ステップ 4 ドロップダウンを使用して、**[デバイス 範囲（Device Scope）]** を選択します。

選択した**[デバイス 範囲（Device Scope）]**で構成されているデバイスが表示されます。

Note デバイスが表示されない場合は、 **Credentials Administration）] > [ログイン情報の管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）のログイン情報（LAN Credentials）]** を選択して、デバイスの ローカル エリア ネットワーク（LAN）のログイン情報が設定されているかどうかを確認します。

ステップ 5 矢印を使用してデバイスをジョブ作成用の右側の列に移動し、**[次へ（Next）]**をクリックします。

ステップ 6 **[変数の定義（Define Variable）]**セクションで、VSAN_ID、VLAN_ID、ETH_SLOT_NUMBER、VFC_SLOT_NUMBER、SWITCH_PORT_MODE、ETH_PORT_RANGE、および ALLOWED_VLANS の値を指定します。

Note 選択したテンプレートに基づいて、変数は異なります。

ステップ 7 **[デバイスごとの変数の編集（Edit Variable Per Device）]** セクションで、フィールドをダブルクリックして特定のデバイスの変数を編集し、**[次へ（Next）]** をクリックします。

ステップ 8 複数のデバイスを選択した場合は、ドロップダウンを使用して特定のデバイスを選択し、その構成をプレビューします。**[戻る（Back）]** をクリックして構成を編集するか、**[次へ（Next）]** をクリックします。

ステップ 9 [ジョブ名と（name and）]説明を指定します。

デバイスのログイン情報は **Credentials Administration）] > [ログイン情報の管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）のログイン情報（LAN Credentials）]** から移入されています。

ステップ 10 ラジオ ボタンを使用して、**[インスタント ジョブ（Instant Job）]** または**[スケジュール ジョブ（Schedule Job）]** を選択します。

[ジョブのスケジュール（Schedule Job）] を選択した場合は、ジョブの配信日時を指定します。

ステップ 11 チェック ボックスを使用して、**[実行を開始にコピー（Copy Run to Start）]** を選択します。

ステップ 12 より多くのトランザクションおよび配信オプションを構成する場合は、チェック ボックスを使用して **[その他のオプションを表示（Show more options）]** を選択します。

ステップ 13 **[トランザクション オプション(オプション)（Transaction Options(Optional)）]** で、ロールバック機能をサポートするデバイスがある場合は、**[ロールバックを有効にする（Enable Rollback）]** チェック ボックスをオンにして、適切なラジオ ボタンを選択します。

適切なラジオ ボタンを選択することによって次のオプションから選択することができます。

- そのデバイスに障害がある場合、デバイスの構成をロールバックする

- 任意のデバイスに障害がある場合、すべてのデバイスの構成をロールバックする
- そのデバイスに障害がある場合、デバイスの構成をロールバックし、残りのデバイスに配信されるさらなる構成を停止する

ステップ 14 **[配信オプション(オプション)]** で、コマンド応答タイムアウトを秒単位で指定し、ラジオ ボタンを使用して配信順序を選択します。コマンド応答タイムアウトの値の範囲は 1 ～ 180 です。

適切なラジオ ボタンを選択することによって次のオプションから選択することができます。

- 一度に 1 つのデバイスの構成を順番に配信する
- 構成をすべてのデバイスに同時に並行して配信する

ステップ 15 **[終了（Finish）]** をクリックして、ジョブを作成します。

ウィザードが正常に完了したことを示す確認メッセージが表示されます。ジョブが **[ジョブ]** ウィンドウに一覧表示されます。

テンプレートの変更

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。

Procedure

ステップ 1 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** から、テンプレートを選択します。

ステップ 2 **[テンプレートの変更/表示（Modify/View template）]** をクリックします。

ステップ 3 テンプレートの説明とタグを編集します。

編集したテンプレートの内容が右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレート チェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート コンテンツ（Template Content）]** ウィンドウで、要件に基づいてテンプレート コンテンツを編集できます。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）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレート構文の検証]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートのコピー

Cisco DCNM Web UI からテンプレートをコピーするには、以下の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択して、テンプレートを選択します。

ステップ 2 **[テンプレートに名前を付けて保存（Save Template As）]** をクリックします。

ステップ 3 テンプレート名、説明、タグ、およびその他のパラメータを編集します。

編集したテンプレートの格納ファイルが右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート格納ファイルは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート 格納ファイル（Template Content）]** ウィンドウで、要件に基づいてテンプレート格納ファイルを編集できます。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）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレートシンタックスの検証（Validate Template Syntax）]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートの削除

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。Cisco DCNM リリース 11.0(1) 以降、複数のテンプレートを一度に削除できます。

Cisco DCNM Web UI からテンプレートを削除するには、以下の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。

ステップ 2 チェックボックスを使用してテンプレートを選択し、**[テンプレートの削除（Remove template）]** アイコンをクリックします。

テンプレートは警告メッセージなしで削除されます。

What to do next

DCNM Web UI のテンプレート リストからテンプレートが削除されます。DCNM サービスを再起動すると、削除されたテンプレートが **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** ページに表示されます。

テンプレートを永久的に削除するには、ローカル ディレクトリ `Cisco Systems\dcm\dcnm\data\templates\` に位置するテンプレートを削除します。

テンプレートのインポート

Cisco DCNM 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 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択し、**[インポート テンプレート（Import Template）]** をクリックします。

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。

必要に応じて、テンプレートパラメータを編集できます。詳細については、テンプレートの変更, on page 191を参照してください。

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。

ステップ 3 **[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 4 **[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。

Note Cisco 定義の FabricPath および IP VXLAN Programmable Fabric POAP テンプレートを Cisco DCNM Web クライアントにインポートできます。詳細については、「*POAP* テンプレートのインストール」を参照してください。

テンプレートのエクスポート

Cisco DCNM Web UI からテンプレートをエクスポートするには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。

ステップ 2 チェック ボックスを使用してテンプレートを選択し、**[テンプレートのエクスポート（Export Template）]** アイコンをクリックします。

ブラウザは、テンプレートを開くか、ディレクトリに保存するように要求します。

POAP テンプレートのインストール

Cisco DCNM 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ー定義テンプレートを追加、編集、または削除できます。Cisco DCNM リリース 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、Cisco 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 DCNM 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 DCNM 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。

Procedure

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。

- `dcnm_ip_vxlan_fabric_templates.10.0.1a.zip`
- `dcnm_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 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。

ステップ 4 **[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 5 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 6 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 7 **[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 8 **[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。

ジョブの構成

Cisco DCNM Web UI からジョブを構成するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Templates Library）] > [ジョブ（Jobs）]** を選択します。

ジョブは、ジョブ識別子、説明、およびステータスとともに一覧表示されます。最新のタスクが一番上に表示されます。

Note ネイティブ HA でフェールオーバーがトリガーされると、ジョブ 識別子 シーケンス番号が 32 ずつ増加します。

ステップ 2 **[フィルタ処理を表示（Show Filter）]** をクリックして、リストをフィルタ処理します。

[ステータス（Status）] 列で、ドロップダウンを使用してジョブのステータスを選択します。

ステップ 3 ジョブを選択し、**[削除（Delete）]** アイコンをクリックしてジョブを削除します。

ステップ 4 ジョブのステータスを表示するには、**[ジョブ識別子（Job ID）]** ラジオボタンをクリックし、**[ステータス（Status）]** をクリックします。

ステップ 5 デバイスのコマンド実行ステータスを表示するには、**[ジョブ実行ステータス（Job Execution Status）]** ウィンドウの **[デバイス（Devices）]** テーブルでデバイス名のラジオ ボタンをクリックします。

Note 複数のジョブを一度に削除できますが、複数のジョブのステータスを一度に表示することはできません。

バックアップ

[バックアップ（Backup）] メニューには次のサブメニューが含まれます。

スイッチの設定

この機能を使用すると、実行構成からデバイス構成をファイル システムの通常のテキスト ファイルとしてバックアップできます。ただし、スタートアップ構成で操作を実行することもできます。バックアップ ファイルは、DCNM サーバー ホストまたはファイル サーバーに保存できます。

選択したデバイス リストのジョブのスケジューリングをサポートするようにアーカイブ システムを構成することもできます。1 つのスイッチに設定できるジョブは 1 つだけです。

次の表は、**[構成] > [バックアップ] > [スイッチ構成]** に表示されるアイコンとフィールドについて説明しています。

表 *17 :* スイッチ構成操作

アイコン	説明
構成をブートフラッシュにコピーします。	スイッチの構成ファイルを、選択した接続先スイッチのブートフラッシュにコピーできます。
設定の表示	構成ファイルを表示または編集できます。
設定の削除	構成ファイルを削除できます。
構成の比較	異なるデバイスまたは同じデバイスの 2 つの構成ファイルを比較できます。
Export Configuration	DCNM サーバーから設定ファイルをエクスポートできます。
ユーザーに定義された構成をインポート	ユーザー定義の構成ファイルを DCNM サーバーにインポートできます。
デバイスへの構成の復元	選択したデバイスから構成を復元できます。
アーカイブ ジョブ	ジョブを追加、削除、表示、または変更できます。

表 *18 :* スイッチ構成のフィールドと説明

フィールド	説明
[デバイス名（Device Name）]	デバイス名を表示します。 デバイスの横にある矢印をクリックして、構成ファイルを表示します。
IP アドレス	デバイスの IP アドレスを表示します。
グループ	デバイスのグループを表示します。
設定	アーカイブされたデバイスの構成ファイルを表示します。

フィールド	説明
アーカイブ時間	デバイス構成ファイルがアーカイブされた時刻を表示します。 フォーマットはDay:Mon:DD:YYYY HH:MM:SSです。
サイズ	アーカイブ ファイルのサイズを表示します。

この項の内容は、次のとおりです。

設定のコピー

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。

Procedure

ステップ 1 Cisco DCNM ホームページから、**[構成（Configure）] > [バックアップ（Backup）] > [スイッチ構成（Switch Configuration）]** を選択します。コピーする必要があるデバイスの起動/実行/アーカイブ構成を選択します。

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

[ブートフラッシュに構成コピー（Copy Configuration to bootflash）] ページが表示され、**[送信元構成のプレビュー（Source Configuration Preview）]** 領域および**[選択したデバイス（Selected Devices）]** 領域が表示されます。

[送信元構成のプレビュー（Source Configuration Preview）] 領域には、デバイスにコピーされた実行/起動/バージョン構成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。

Note 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。

[構成の表示（View Configuration）]

デバイスにあるの構成ファイルを表示または、編集できます。

デバイスにあるの構成ファイルを表示または編集するために、次のタスクを実行します。

Procedure

ステップ 1 Cisco DCNM ホーム ページから **[構成] > [バックアップ] > [スイッチ構成（Switch Configuration）]** を選択します。デバイス名の横にある矢印をクリックして、デバイスの構成ファイルを表示します。構成ファイルを表示には、構成ファイルのラジオ ボタンを選択します。

ステップ 2 [構成の表示 をクリックします。

表示設定画面が表示され、構成ファイルの内容が表示されます。

設定の削除

デバイスから構成ファイルを削除するには、次のタスクを実行します。

Note 構成ファイルを削除する前に、必ずバックアップを取ってください。

Procedure

ステップ 1 Cisco DCNM ホーム ページから **[構成 > バックアップ > スイッチ構成（Configure > Backup > Switch Configuration）]** を選択します。デバイス名の横にある矢印をクリックして、デバイスの構成ファイルを表示します。

ステップ 2 削除する構成ファイルラジオボタンをクリックします。

Note 複数の構成ファイルを削除できます。ただし、スタートアップ、または実行コンフィギュレーション ファイルは削除できません。

ステップ 3 構成ファイルを削除するために、 **[はい（Yes）]** をクリックします。

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。

Procedure

ステップ 1 **[構成 > バックアップ > スイッチ構成（Configure > Backup > Switch Configuration）]** に移動します。デバイス名の横にある矢印をクリックして、デバイスの構成ファイルを表示します。

ステップ 2 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 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）]**：[削除された設定の詳細。（Deleted configuration details.）]
- **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。
- [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

Cisco DCNM サーバから構成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。

Procedure

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

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。

コンフィギュレーションファイルをインポート

ファイル サーバから Cisco DCNM に構成ファイルをインポートできます。

1 つまたは複数の構成ファイルをインポートするには、次のタスクを実行します。

Procedure

ステップ 1 Cisco DCNM ホーム ページから **[構成（Configure）] > [バックアップ（Backup）] > [スイッチ構成（Switch Configuration）]** を選択し **[ユーザーに定義済みの構成（Import User-Defined Configuration）]** をクリックします。

ファイル サーバ ディレクトリが開きます。

ステップ 2 ディレクトリを参照し、インポートする構成ファイルを選択します。[開く（Open）]をクリックします。

確認の画面が表示されます。

Note ファイル名には、スラッシュ（/）または円記号（\）を含めないでください。

ファイル名は任意の英数字ストリングです。ピリオド（.）、下線（_）、およびスペースを含めることもできます。.cfg 拡張子を持つファイルのみをインポートできます。

ステップ 3 **[はい（Yes）]** をクリックして、選択したファイルをインポートします。

インポートされた構成ファイルは、ユーザーがインポートしたファイルとして表示されます。

構成の復元

選択したスイッチまたは 構成ファイルを復元できます。[Cisco DCNM リリース 11.0（1）以降では、選択した日付に基づいて設定を復元することもできます。（From Cisco DCNM Release 11.0（1）, you can restore configuration based on the selected date as well.）]

Note SAN スイッチおよび FCoE 対応スイッチの構成は復元できません。

選択したデバイスから構成を復元できます。

Procedure

ステップ 1 Cisco DCNM ホーム ページから **[構成（Configure ）] > [バックアップ（Backup）] > [スイッチ構成（Switch Configuration）]** を選択し**[復元（Restore）]**をクリックします。

ステップ 2 ドロップダウン リストから、該当する復元のタイプを選択します。**[バージョンベース（Version-based）]**または**[日付ベース（Date-based）]**を選択できます。

Note
- 日付ベースの復元を選択した場合は、日付と時刻を選択する必要があります。上記の時刻より前に使用可能な構成が復元されます。
- バージョンベースの復元を選択した場合は、**[構成（Configuration）]**列から構成を選択する必要があります。**[表示（View）]** 列で構成の詳細を表示できます。

ステップ 3 構成を復元する**[デバイス名（Device Name）]**のチェックボックスをオンにします。[復元（Restore）] をクリックします。

[デバイス（Devices）] エリアは次のフィールドを表示します。

- デバイス名 — 復元した構成ファイルのデバイス名を指定します。
- IP アドレス — 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。

Note 同じデバイスからのみ構成を復元できます。ユーザーがインポートした構成ファイルを選択すると、任意の数のデバイスの構成を復元できます。

アーカイブ ジョブ

このセクションには、**[構成 > バックアップ（Configure > Backup）][スイッチ構成（Switch Configuration）] >[アーカイブ ジョブ（Archive Jobs）]** にある状況依存のオンライン ヘルプ コンテンツが含まれています。

DCNM スイッチ アーカイブ ジョブでは、SNMPv3 が要件としてリストされています。ジョブ実行時のエラー原因が「スイッチが SNMPv3 で管理されていない（Switch is not managed using SNMPv3）」、ステータスが「不適格（Not Eligible）」です。これは文書化されていません。

（注） アーカイブされたジョブの設定ファイルは、DCNM サーバ ディレクトリにあります。\dcm\dcnm\data\archive\<dcnm-ip-address> \ サードパーティのファイル転送ツールまたはファイル転送コマンドを使用して、これらのファイルを外部サーバーに転送できます。

次のテーブルでは、**[アーカイブ ジョブ（Archive Jobs）]** ウィンドウに表示されるフィールドを説明します。

フィールド	説明
ユーザ	このジョブの作成者を指定します。
グループ	ジョブが属するグループを指定します。
グループ ジョブ	グループ ジョブかデバイスごとのジョブかを指定します。値は **[true]** または **[false]** です。
スケジュール	ジョブのスケジュールを指定します。繰り返しの情報も表示します。
前回の実行	このジョブが最後に実行された日時を指定します。
[ジョブ ステータス（Job Status）]	ジョブが成功したか、スケジュールされたか、実行中か、失敗したかを指定します。 （注） **実行中（Running）** および **スケジュール済み（Scheduled）** ステータスは、アップグレードされた Cisco DCNM の既存のジョブには適用されません。 ステータスが **[不適格]** と表示され、エラーが表示される DCNM で SNMPv3 が有効になっていない場合、**スイッチは SNMPv3 を使用して管理されていません。**
ユーザコメント	ユーザーが提供するコメントまたは説明を指定します。

アーカイブ ジョブ

Cisco DCNM Web UI からジョブを追加、削除、表示するには、次の手順を実行します。

Note ジョブを構成する前に、SFTP/TFTP/SCP ログイン情報を設定する必要があります。DCNM Web クライアントで、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] >[アーカイブ FTP ログイン情報]** に移動して、ログイン情報を設定します。

Procedure

ステップ 1 **[構成Configure）] > [バックアップ（Backup）] > [スイッチ構成（Switch Configuration）] > [アーカイブ ジョブ（Archive Jobs）] > [アーカイブ ジョブ（Archive Jobs）]** タブを選択し、**[ジョブの追加（Add Job）]** をクリックします。

[ジョブの作成]画面には、スケジュール、デバイスの選択、および選択されたデバイスが表示されます。

バックアップは定義どおりにスケジュールされます。

a) **[スケジュール]** 領域で、開始時刻、繰り返し間隔、および繰り返し日を構成します。

- 開始時刻: 時間:分:秒のドロップダウン リストを使用して開始時刻を構成します。
  - **1 回**：特定の日に 1 回実行されるようにジョブを構成します。このジョブが実行される時刻は、**[開始時刻]** フィールドによって決定されます。
  - 今すぐ - ジョブをすぐに実行するように構成します。Cisco DCNM は、サーバーで構成されているデフォルトの日時を考慮します。

    Note ジョブがすでにスケジュールされている場合でも、ジョブを**今すぐ**実行するようにスケジュールできます。

  - **毎日**：このジョブを実行する曜日のチェック ボックスをオンにします。このジョブが実行される時刻は、**[開始時刻]** フィールドによって決定されます。
  - **リアルタイム**：デバイスで構成が変更された場合に実行されるジョブを構成します。DCNM サーバーがこのジョブを実行した後、デバイスは 5 分間静止している必要があります。
- **繰り返し間隔** : スケジュールされた間隔でジョブを繰り返すには、[繰り返し間隔] チェック ボックスをオンにします。日または時間のドロップダウン リストを使用して間隔を構成します。
- **コメント** : コメントがあれば入力します。

b) **[デバイスの選択]** 領域で、ラジオ ボタンを使用して次のいずれかを選択します。

- **デバイス グループ** : [デバイス グループ] ラジオ ボタンをクリックして、このジョブのデバイス グループ全体を選択します。

  ドロップダウン リストから、必要なデバイス グループを選択します。

Note デバイスにライセンスが付与されていない場合、それらはCisco DCNMの **[構成] > [バックアップ] > [スイッチの構成] > [アーカイブ ジョブ]** のグループの下に表示されません。グループ内のどのデバイスにもライセンスが付与されていない場合、そのグループ内のデバイスにライセンスが付与されるまで、グループのみがデバイスなしで表示されます。

- **選択されたデバイス**：**[選択されたデバイス]** ラジオボタンをクリックして、このジョブのさまざまなグループから複数のデバイスの 1 つを選択します。

  ドロップダウンリストから [デバイス] を選択します。

  Cisco DCNM リリース 11.2(1) 以降、選択したすべてのデバイスに同時に VRF を適用できます。管理 VRF またはデフォルト VRF のいずれかを適用できます。

Note スイッチに SAN および LAN ログイン情報が構成されていない場合、そのスイッチは [選択されたデバイス] ドロップダウンリストに表示されません。設定するには、**[管理] > [SAN クレデンシャル][管理] > [クレデンシャル管理] > [LAN クレデンシャル]** に移動します。

c) **[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。

- **名前**：ジョブがスケジュールされているデバイスの名前を指定します。
- **IP アドレス**：デバイスの IP アドレスを指定します。
- **グループ**：デバイスが属しているグループ。
- **VRF**：仮想ルーティングおよび転送（VRF）インスタンスを指定します。

  VRF タイプを選択して、既存の VRF タイプを指定されたデバイスに変更します。管理 VRF またはデフォルト VRF のいずれかを適用できます。

Note デバイスのジョブがデバイス レベルに存在する場合、このスイッチをそのグループの一部として含むグループ レベルのジョブを作成できます。ただし、ジョブの実行中はこのスイッチは除外されます。

d) **[作成]** をクリックして新しいジョブを追加します。

ステップ 2 ジョブを削除するには、Cisco DCNM ホームページから、**[構成] > [バックアップ] > [スイッチ構成] > [ジョブのアーカイブ] > [ジョブのアーカイブ]** を選択し、ジョブを選択します。

a) **[ジョブの削除]** をクリックします。

このジョブのスケジュール、デバイスの選択、および選択されたデバイスが表示されます。

b) [削除（Delete）] をクリックします。

ステップ 3 ジョブの詳細を表示するには、Cisco DCNM ホームページから、**[構成] > [バックアップ] > [スイッチ構成] > [ジョブのアーカイブ] > [ジョブのアーカイブ]** を選択し、[ジョブ] チェックボックスをオンにします。

a) **[ジョブの表示/変更]** をクリックします。

このジョブのスケジュール、デバイスの選択、および選択されたデバイスが表示されます。

b) 必要に応じて詳細を変更します。**[OK]** をクリックして元に戻し、ジョブのリストを表示します。

Note
- **今すぐ**実行するようにスケジュールされているジョブを、**毎日**実行するようにスケジュールされているジョブに変更することはできません。
- アーカイブ ジョブの繰り返し間隔は変更できません。変更しようとすると、操作は失敗し、ジョブは削除されます。既存の繰り返し間隔アーカイブ ジョブを削除して、新しいジョブを作成する必要があります。

What to do next

デバイスごとにアーカイブ ファイルの数を保持するように Cisco DCNM を設定することもできます。**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバーのプロパティ（Server Properties）]** を選択して、**archived.versions.limit** フィールドを更新します。

ジョブ実行の詳細

[Cisco **DCNM Web Client] > [構成（Configure）] > [バックアップ（Backup）] > [スイッチ構成（Switch Configuration）] > [ジョブのアーカイブ（Archive Jobs）] > [ジョブのアーカイブ（Archive Jobs）] > [ジョブ実行の詳細（Job Execution Details）]** タブには、[ジョブ実行の履歴（Job Execution History）] テーブルに次のタブが表示されます。

フィールド	説明
[ジョブ名（Job Name）]	システム生成ジョブ名を表示します。
ユーザ	ジョブを作成した人のペルソナを指定します。
デバイス グループ（Device Group）	ジョブが作成されたファブリックまたはLANグループを指定します。
デバイス	デバイスの IP アドレスを指定します。
サーバー	デバイスが関連付けられている DCNM サーバの IP アドレスを指定します。
プロトコル	SFTP、TFTP、または SCP プロトコルが適用されるかどうかを指定します。
実行時間	ジョブが最後に実行された時刻を指定します。

フィールド	説明
ステータス（Status）	ジョブのステータスを指定します。 • 省略（Skipped） • エラー • 成功
エラーの原因	ジョブが失敗した場合のエラーを指定します。カテゴリは次のとおりです。 • 構成に変更はありません。 • スイッチはこのサーバによって管理されていません。 **Note** エラー原因の列が空の場合、ジョブが正常に実行されたことを意味します。 エラーの原因にカーソルを合わせると、完全な説明が表示されます。

アーカイブ

ネットワーク オペレータ ロールを持つユーザーは、スイッチの設定アーカイブとその詳細を **[アーカイブ（Archives）]** ウィンドウで表示できます。

次の表に、このウィンドウに表示されたアイコンとフィールドの説明を示します。

表 *19 :* アーカイブ操作

アイコン	説明
比較	異なるデバイスまたは同じデバイスの 2 つの構成ファイルを比較できます。
[表示（View）]	構成ファイルを表示できます。

表 *20 :* アーカイブのフィールドと説明

フィールド名	説明
デバイス名（Device Name）	デバイス名を表示します。 デバイスの横にある矢印をクリックして、構成ファイルを表示します。
IP アドレス（IP Address）	デバイスの IP アドレスを表示します。

フィールド名	説明
グループ	デバイスのグループを表示します。
設定	そのデバイス用にアーカイブされた構成ファイルが表示されます。
アーカイブ時間	デバイス構成ファイルがアーカイブされた時刻を表示します。 形式は Day:Mon:DD:YYYY HH:MM:SS です。
サイズ	アーカイブされたファイルのサイズを表示します。

この項の内容は、次のとおりです。

設定ファイルの比較

構成ファイルの 1 つのバージョンを、同じデバイス内の同じ構成ファイルの別のバージョン、または 2 つの異なるデバイスの構成ファイルと比較できます。

Cisco DCNM Web UI から構成ファイルを比較するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [バックアップ（Backup）] > [アーカイブ（Archives）]** を選択します。

ステップ 2 **[アーカイブ]** 領域で、構成ファイルを表示するデバイスの名前の横にある矢印をクリックします。構成ファイルのリストが表示されます。

ステップ 3 構成ファイルの隣にあるチェックボックスを選択し、比較する 2 つの構成ファイルを選択します。

選択する最初のファイルは、送信元として指定され、2 番目の設定ファイルは宛先ファイルとして指定されます。

ステップ 4 [比較（Compare）] をクリックします。

[構成差分の表示（View Config Diff）] ページは、2 つの構成ファイル間の違いを表示します。

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

構成ファイルの違いは、凡例とともに表に示されています。

- **[赤（Red）]**：[削除された構成の詳細（Deleted configuration details.）]
- **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。

構成の表示

アーカイブされた構成ファイルを表示することも。

Cisco DCNM Web UI からデバイスの構成ファイルを表示または編集するには、以下の手順を実行します：

Procedure

ステップ 1 **[構成（Configure）] > [バックアップ（Backup）] > [アーカイブ（Archives）]** を選択します。

[アーカイブ（Archives）]ウィンドウが表示されます。

ステップ 2 構成ファイルを表示するデバイスの名前の横にある矢印をクリックします。

構成ファイルのリストが表示されます。

ステップ 3 表示する対応ファイルの横にあるラジオ ボタンを選択します。

ステップ 4 **[表示（View）]** 構成アイコンをクリックします。

[表示（View）]構成ウィンドウが表示され、右側の列に構成ファイルの内容が表示されます。

ネットワーク構成の監査

Cisco DCNM は、ネットワーク スイッチ全体の構成変更の監査を提供します。ネットワーク監査レポート機能を使用すると、追加、削除、または変更された構成を追跡できるように監査レポートを生成できます。既存のアーカイブ ジョブがある場合にのみ、ネットワーク監査レポートを生成できます。生成されたレポートを使用して、指定された期間のデバイスの構成の違いを表示できます。

この項の内容は、次のとおりです。

ネットワーク構成監査レポートの生成

Cisco DCNM Web UI からネットワーク構成監査レポートを生成するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [バックアップ（Backup）] > [ネットワーク構成監査（Network Config Audit）]** を選択します。

[ネットワーク監査レポート（Network Audit Report）] ウィンドウが表示されます。

ステップ 2 **[デバイス（Device）]** ドロップダウン リストで、レポートを生成するデバイスを選択します。

ステップ 3 **[開始日（Start Date）]**と**[終了日（End Date）]**を指定します。

ステップ 4 **[レポートの生成（Generate Report）]** をクリックして、構成の違いを表示します。構成の違いは色分けされています。

- 赤：削除された構成
- 緑：新しく追加された構成
- 青：変更された構成
- 取り消し線：古い構成

レポートを生成したら、構成レポートを HTML ファイルにエクスポートできます。

ネットワーク構成監査レポートの作成

ネットワーク構成監査ジョブを作成し、Cisco DCNM Web UI からデバイス間の構成の違いを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [レポート（Report）] > [生成（Generate）]** を選択します。

左ペインには、作成できるさまざまなレポートが表示されます。

ステップ 2 **[共通（common）] > [ネットワーク構成監査（Network Config Audit）]** を選択します。

ステップ 3 **[レポート名（Report Name）]** フィールドに、レポートの名前を入力します。

ステップ 4 **[繰り返し（Repeat）]** フィールドで、適切な繰り返し間隔(毎日、毎週、または毎月) を選択します。

日次ジョブは、選択したすべてのデバイスについて、過去1日間の構成の違いに関するレポートを生成します。週次ジョブは過去 7 日間のレポートを生成し、月次ジョブは過去 30 日間のレポートを生成します。

ステップ 5 **[開始日（Start）]** フィールドと **[終了日（End）]** フィールドで、レポートの開始日と終了日を指定します。

ステップ 6 **[電子メール レポート（Email Report）]** フィールドで、電子メール配信オプションを指定します。

- いいえ：レポートを電子メールで送信しない場合は、このオプションを選択します。
- リンクのみ：レポートへのリンクを送信する場合は、このオプションを選択します。
- 内容：レポートの内容を送信する場合は、このオプションを選択します。

リンクのみまたはコンテンツオプションを選択した場合は、**[宛先（To）]** フィールドと **[件名（Subject）]** フィールドに電子メール アドレスと件名を入力します。

ネットワーク構成監査レポートのモニタリング

Cisco DCNM Web UI からネットワーク構成監査レポートをモニタするには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [レポート（Report）] > [表示（View）]** を選択します。

ステップ 2 左側のペインで **[共通（Common）] > [ネットワーク構成監査（Network Config Audit）]** を選択して、ネットワーク構成監査レポートを表示します。

ネットワーク構成監査レポートの削除

Cisco DCNM Web UI からネットワーク構成監査レポートを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [レポート（Report）] > [表示（View）]** を選択します。

ステップ 2 **[共通（common）] > [ネットワーク構成監査（Network Config Audit）]** を選択します。

[レポートの表示（View Reports）] ウィンドウに、作成したレポートが表示されます。

ステップ 3 削除するレポートを選択し、**[削除（Delete）]** アイコンをクリックします。

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 [と Cisco MDS スイッチ（and Cisco MDS switches）]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）] メニューには、次のサブメニューが含まれています：

[アップグレード [ISSU]（Upgrade [ISSU]）]

[アップグレード [ISSU]（Upgrade [ISSU]）] メニューには、次のサブメニューが含まれています。

アップグレード履歴 [ISSU]

この機能により、In-Service Software Upgrade（ISSU）を使用して Cisco Nexus プラットフォーム スイッチをアップグレードできます。このアップグレード手順は、デバイス構成に基づいて、中断を伴う場合もあれば、中断しない場合もあります。アップグレードに必要なキックスタート、システム、またはイメージは、SFTP、SCP、TFTP、FTP を使用してリモート サーバーから、またはデバイス上のイメージ リポジトリまたはファイル システムから選択できます。イメージ リポジトリは、ファイル転送プロトコルとして SCP、SFTP、FTP、または TFTP を使用できます。リポジトリからイメージを選択するには、**[構成] > [イメージ管理] > [リポジトリ]** タブから同じイメージをアップロードする必要があります。

次の表では、**[構成] > [イメージ管理] > [アップグレード [ISSU]] > [アップグレード履歴]** 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
タスク ID（Task Id）	タスクのシリアル番号を指定します。最新のタスクが上部に表示されます。 **Note** ネイティブ HA でフェールオーバがトリガされると、タスク ID シーケンス番号が 32 ずつ増加します。
タスクタイプ	タスクのタイプを指定します。 • 互換性 • アップグレード
オーナー	Role-Based Authentication Control（RBAC）に基づいて、このタスクを開始した所有者を指定します。
Devices	このタスク用に選択されたすべてのデバイスを表示します。

フィールド	説明
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了） • 例外ありで完了 **Note** ジョブが 1 つまたは複数のデバイスで失敗した場合、ステータス フィールドには失敗を示す COMPLETED WITH EXCEPTION が表示されます。
作成時刻	タスクが作成された時間を指定します。
スケジュール	タスクの実行を指定する時刻を指定します。タスクを後で実行するようにスケジュールすることもできます。
完了時刻	タスクが完了した時間を指定します。
備考	タスクの実行中に所有者が追加したコメントを表示します。

Note Cisco DCNM の新規インストール後、このページにはエントリがありません。

次を実行します。

新しいインストール

Cisco DCNM から検出されたデバイスをアップグレードするには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU]）] > [アップグレード履歴（Upgrade History）]**を選択します。

ステップ 2 **[新しいインストール（New Installation）]** > を選択して、デバイス上のキックスタートおよびシステム イメージをインストールまたはアップグレードします。

デフォルトの VDC を持つデバイスが **[スイッチの選択（Select Switches）]** ウィンドウに表示されます。

ステップ 3 スイッチ名の左側にあるチェック ボックスをオンにします。

複数のスイッチを選択して、スイッチを右の列に移動できます。

ステップ 4 **[追加]** または **[削除]** アイコンをクリックして、アップグレードに適切なスイッチを含めます。

選択したスイッチが右側の列に表示されます。

ステップ 5 [次へ（Next）] をクリックします。

[ISSU 前後のレポート（Pre-Post ISSU Reports）] ウィンドウが表示されます。

Note プレポスト ISSU レポートは、SAN およびメディア コントローラのインストールではサポートされていません。

ステップ 6 [次へ（Next）] をクリックします。

[ソフトウェア イメージの指定（Specify Software Images）] ウィンドウが表示されます。このタブには、前の画面で選択したスイッチが表示されます。アップグレードするイメージも選択できます。

- **[自動ファイル選択]** チェック ボックスを使用すると、ファイル サーバー、イメージ バージョン、およびアップグレードされたイメージを選択したデバイスに適用できるパスを指定できます。
- **[ファイル サーバーの選択（Select File Server）]** ドロップダウン リストで、Cisco DCNM リポジトリに作成されたファイル サーバーの 1 つを選択します。
- **[イメージ バージョン]** フィールドで、イメージのバージョンを指定します。たとえば、**イメージ バージョン**として m9700-sf3ek9-kickstart-mz.7.3.0.D1.1.bin を選択した場合は、[イメージ バージョン] フィールドに 7.3.9.D1.1 と入力します。
- **[パス（Path）]** フィールドに、イメージパスを入力します。SCP または SFTP を選択した場合は、絶対パスを指定します。たとえば、//root/images/ です。FTP または TFTP を選択した場合は、FTP または TFTP ホーム ディレクトリへの相対パスを指定します。Cisco DCNM によって提供される TFTP サーバー、ローカル DCNM TFTP を使用している場合は、イメージの絶対パスを指定します。現在のジョブが進行中の場合、別のジョブを作成するために同じ DCNM TFTP サーバーを使用することはできません。

ステップ 7 **[キックスタート イメージ]** 列で **[イメージを選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

Note
- Cisco Nexus 3000 シリーズおよび 9000 シリーズ スイッチでは、Cisco NX-OS オペレーティング システムをロードするためにシステム イメージのみが必要です。したがって、これらのデバイスのキックスタートイメージを選択するオプションは無効になっています。
- **[ソフトウェア イメージ ブラウザ]** ダイアログ ボックスの表示に問題がある場合は、ブラウザのフォント サイズを小さくして再試行してください。

ステップ 8 **[システム イメージ]** 列で **[イメージの選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

ステップ 9 **[ソフトウェア イメージ ブラウザ（Software Image Browser）]** ダイアログボックスで、**[ファイル サーバー（File Server）]** または **[スイッチ ファイル システム（Switch File System）]** からイメージを選択できます。

ファイル サーバーを選択した場合：

a) **[ファイル サーバーの選択]** リストから、イメージが保存されている の適切なファイル サーバーを選択します。

[構成] > [イメージ管理] > [リポジトリ] のサーバーがドロップダウン リストに表示されます。

b) **[画像の選択]** リストから、適切な画像を選択します。同じプラットフォームの他のすべての選択したデバイスに同じイメージを使用するには、チェック ボックスをオンにします。

例：プラットフォーム タイプ N7K-C7009 および N7K-C7010 の場合、ロジックはプラットフォーム（N7K）とサブプラットフォームの 3 文字（C70）に一致します。すべてのプラットフォーム スイッチで同じロジックが使用されます。

Note **ファイル サーバー**を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

c) [VRF の選択（**Select Vrf**）] ドロップダウン リストから VRF を選択します。

Note このフィールドは、Cisco MDS スイッチには表示されません。

この VRF は、他の選択されたデバイスに対してデフォルトで選択されています。デフォルト値は **[management]** です。

d) [OK] をクリックします。

選択したファイル サーバーが `ftp` または `tftp` の場合、テキスト ボックスに、ホーム ディレクトリからのファイルの相対パスを入力します。

このイメージは、同じプラットフォーム タイプの他のすべての選択されたデバイスに対して選択されます。

[ファイル システムの切り替え] を選択した場合：

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なイメージを選択します。

Note **スイッチ ファイル システム（Switch File System）]** を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックしキックスタート イメージを選択するか、**[キャンセル（Cancel）]** をクリックして **[ソフトウェア イメージの指定（Specify Software Images）]** ダイアログ ボックスに戻ります。

ステップ 10 **[Vrf]** 列では、仮想ルーティングおよびフォワーディング（VRF）の名前を示します。

VRF は Cisco MDS デバイスには適用されません。

ステップ 11 **[使用可能なスペース（Available Space）]** 列で、スイッチの**プライマリ スーパーバイザ** モジュールと**セカンダリ スーパーバイザ** モジュールに使用可能なスペースを指定します。

[使用可能なスペース] 列には、スイッチで使用可能なメモリが MB で表示されます (1 MB 未満の場合は、KB として表示およびマークされます。

ブートフラッシュ ブラウザでは、スイッチ ブートフラッシュにあるすべてのファイルとディレクトリのファイル名、サイズ、最新の変更日を表示します。ファイルを削除するには、ファイルを選択して **[削除]** をクリックし、スイッチの空き容量を増やします。

ステップ 12 **[選択されたファイルのサイズ]** 列には、SCP または SFTP サーバーから選択されたイメージのサイズが表示されます。

選択したイメージの合計サイズがスイッチの使用可能なスペースより大きい場合、ファイルサイズは赤でマークされます。スイッチにイメージをコピーしてインストールするためのスペースを増やすことをお勧めします。

ステップ 13 スイッチをドラッグ アンド ドロップして、アップグレード タスク シーケンスを並べ替えます。

ステップ 14 (Optional) デバイス上の Cisco NX-OS ソフトウェア バージョンと、選択したアップグレードされたイメージとの互換性をチェックする場合は、**[バージョンの互換性をスキップ（Skip Version Compatibility）]** チェックボックスをオフにします。

ステップ 15 すべてのラインカードを同時にアップグレードするには、**[パラレル ライン カードのアップグレードの選択（Select Parallel Line Card upgrade）]** を選択します。

パラレル ライン カードのアップグレードは、Cisco MDS デバイスには適用されません。

ステップ 16 **[アップグレード オプション]** 列の **[オプション]** をクリックして、アップグレードのタイプを選択します。

[アップグレードオプション] ウィンドウに2つのアップグレードオプションが表示されます。**アップグレード オプション 1** のドロップダウン リストには、次のオプションがあります。

- **中断**
- **Bios force**
- **無停止を許可**

- 無停止を強制

中断は、Cisco Nexus 9000 シリーズ スイッチのデフォルト値です。アップグレード オプションは、他のスイッチには**適用されません**。

[アップグレード オプション1] の下で **[無停止を許可（Allow Non Disruptive）]** を選択し、スイッチが無停止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。

アップグレード オプション 1 で **[無停止を強制（Force non-disruptive）]** を選択すると、互換性チェックが無停止アップグレードに必須であるため、**[バージョン互換性の確認（Skip Version Compatibility）]** チェック ボックスがオフになります。選択したスイッチが無停止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。

[アップグレード オプション 2] のドロップダウン リストには、**[アップグレード オプション 1]** で **[無停止を許可]** または **[無停止を強制]** を選択すると、次のオプションがあります。

- 北米
- バイオスフォース

アップグレード オプション 1 で **Disruptive** または **Bios-force** を選択すると、**アップグレード オプション 2** では **アップグレード オプション 2** は無効になります。

選択したすべてのデバイスに選択したオプションを使用するには、**[他のすべての選択したデバイスにこのオプションを使用する]** チェック ボックスをオンにして、**[OK]** をクリックします。

Note
- アップグレード オプションは、Cisco Nexus 3000 シリーズおよび 9000 シリーズ スイッチにのみ適用されます。
- アップグレードに **[無停止を許可]** オプションを選択しても、無停止アップグレードが保証されるわけではありません。互換性チェックを実行して、デバイスが無停止アップグレードをサポートしていることを確認します。

ステップ 17 [次へ（Next）] をクリックします。

[バージョンの互換性をスキップ] を選択しなかった場合、Cisco DCNM は互換性チェックを実行します。

チェックが完了するまで待つか、**[後でインストールを終了]** をクリックするかを選択できます。

インストール ウィザードが閉じられ、互換性タスクが **[構成] > [イメージ管理] > [アップグレード [ISSU]] > [アップグレード履歴]** で作成されます。

イメージの互換性のチェックにかかる時間は、構成とデバイスの負荷によって異なります。

バージョン互換性検証互換性検証 ステータス列には、検証のステータスが表示されます。

[バージョン互換性をスキップ（Skip Version Compatibility）] を選択してバージョン互換性チェックをスキップすると、Cisco DCNM はデバイスの名前だけを表示します。**[現在のアクション]**列には**[完了]**と表示され、**互換性検証]**列には**[スキップされました]**と表示されます。

スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 18 **[後でインストールを終了]** をクリックして、後でアップグレードを実行します。

ステップ 19 [次へ（Next）] をクリックします。

ステップ 20 **[次へ]**チェックボックスをオンにして、アップグレードの前にデバイスをメンテナンスモードにします。

ステップ 21 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 22 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MMM/DD/YYYY HH:MM:SS 形式で指定します。

時刻はサーバーに相対的です。選択した展開時刻が過去の場合、ジョブはすぐに実行されます。

ステップ 23 アップグレード対象として選択したデバイスとラインカードに基づいて、実行モードを選択できます。

a. **[順次]** を選択して、選択した順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 24 **[終了（Finish）]** をクリックし、アップグレード プロセスを開始します。

インストール ウィザードが閉じ、**[構成] > [イメージ管理] > [アップグレード [ISSU]] > [アップグレード履歴]** ページにアップグレードするタスクが作成されます。

What to do next

スイッチで ISSU を完了したら、スイッチが再起動し、SNMP エージェントが安定するまで 20 分間待機します。DCNM は、Cisco DCNM Web UI にスイッチの新しいバージョンを表示するために、投票サイクルを検出します。

インストールの終了

[互換性チェック（Compatibility Check）] ページで完了したタスクのインストールを完了することを選択できます。次のタスクを実行して、デバイスのアップグレードプロセスを完了します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU]）] > [アップグレード履歴コントロール（Upgrade History** を選択し、互換性チェックが完了したタスクを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 **[インストールの終了（Finish Installation）]** をクリックします。

[ソフトウェア インストール ウィザード（Software Installation Wizard）] が表示されます。

ステップ 3 スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 4 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 5 チェックボックスをオンにして、アップグレードの前にデバイスをメンテナンス モードにします。このオプションは、メンテナンス モードをサポートするデバイスに対してのみ有効です。

ステップ 6 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MM/DD/YYYY HH:MM:SS フォーマットで指定します。

ステップ 7 アップグレード対象として選択したデバイスとラインカードに基づいて、実行モードを選択できます。

a. **[順次（Sequential）]** を選択して、選択された順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時（Concurrent）]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 8 **[終了（Finish）]** をクリックして、アップグレード プロセスを完了します。

表示

Cisco DCNM Web UI からイメージ アップグレード履歴を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU]）] > [アップグレード履歴（Upgrade History）]** を選択し、[タスク 識別子] チェックボックスを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 [表示（View）] をクリックします。

[インストール タスクの詳細（Installation Task Details）] ウィンドウが表示されます。

ステップ 3 [設定（Settings）] をクリックします。**[列（Columns）]** メニューを展開し、表示する詳細を選択します。

このウィンドウには次の情報が表示されます。

- キックスタートとシステム イメージのローケーション
- 互換性チェック ステータス
- インストールステータス
- 説明
- ログ

ステップ 4 デバイスを選択します。

タスクの詳細ステータスが表示されます。完了したタスクについては、デバイスからの応答が表示されます。

アップグレード タスクが進行中の場合は、インストール プロセスのライブ ログが表示されます。

Note
- このウィンドウが表示されている場合、このテーブルは、進行中のジョブについて 30 秒ごとに自動更新されます。
- Cisco MDS スイッチで進行中のアップグレードのスイッチ レベルのステータスは、SAN 資格情報を持たない他のユーザーには表示されません。SAN 資格情報を適用するには、**[管理（Administration）] > [資格情報管理(Credentials Management）] > [SAN 資格情報（SAN Credentials）]** を選択します。

削除

Cisco DCNM Web UI からタスクを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU]）] > [アップグレード履歴（Upgrade History）]**を選択し、**[タスク ID（Task ID）]** チェックボックスを選択します。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 **[OK]** をクリックして、ジョブの削除を確認します。

スイッチ レベルの履歴

アップグレードプロセスの履歴をスイッチ レベルで表示できます。スイッチの現在のバージョンとその他の詳細を表示できます。

次の表では、**[構成（Configure）] > [画像管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU] ）] > [スイッチ レベル履歴（Switch Level History）]** 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	スイッチの IP アドレスを指定します
プラットフォーム [英語]	Cisco Nexus スイッチ プラットフォームを指定します
現在のバージョン	スイッチ ソフトウェアの現在のバージョンを指定します。

スイッチ名の横にあるラジオボタンをクリックしてスイッチを選択し、そのアップグレード履歴を表示します。**[表示（View）]** をクリックして、選択したスイッチのアップグレード タスク履歴を表示します。

次の表では、**[構成（Configure）] > [画像管理（Image Management）] > [[ISSU] のアップグレード（Upgrade [ISSU]）] > [スイッチ レベル履歴（Switch Level History）] > [デバイスのアップグレード タスクの表示（View Device Upgrade Tasks）]** 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
オーナー（Owner）	アップグレードを開始した所有者を指定します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了）
キックスタート画像	スイッチのアップグレードに使用するキックスタート イメージを指定します。

フィールド	説明
システムのイメージ（System Image）	スイッチのアップグレードに使用するシステム画像を指定します。
完了時刻	アップグレードが正常に完了した日時を指定します。
ステータスの説明	ジョブのインストールログ情報を指定します。

パッチ [SMU]

パッチ [SMU] メニューには次のサブメニューが含まれます。

インストール履歴

この機能により、ソフトウェア メンテナンス アップデート（SMU）を使用してパッケージをアクティブ化または非アクティブ化できます。管理者権限を持つ担当者は、この操作を実行できます。

次のテーブルは、 **[構成（Configure）] > [画像管理（Image Management）] > [パッチ [SMU]（Patch [SMU]）] > [インストール履歴（Installation History）]**に現れるフィールドを説明します。

フィールド	説明
タスク ID（Task Id）	タスクのシリアル番号を指定します。最新のタスクが上部に表示されます。 タスクは順番に実行されます。
スイッチ名	パッチ ファイルがインストールされているスイッチの名前を指定します。
IP アドレス	デバイスの IP アドレスを指定します。
タスク	パッチがこのデバイスにインストールされているかアンインストールされているかを指定します。
パッケージ	パッチ ファイルの名前を指定します。
ステータス（Status）	パッチ ファイルのインストールまたはアンインストールのステータスを指定します。
ステータスの説明	パッチ ファイルのインストールまたはアンインストールのステータスを説明します。

この項の内容は、次のとおりです。

パッチのインストール

Cisco DCNM Web クライアントからデバイスのパッチをインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [パッチ [SMU]（Patch [SMU]）] > [インストール履歴（Installation History）]** を選択し、**[インストール（ Install）]** をクリックします。

[スイッチの選択（Select Switches）] ウィンドウが表示されます。Cisco DCNM によって検出されたすべての Cisco Nexus スイッチが表示されます。

ステップ 2 スイッチ名の左側にあるチェック ボックスをオンにします。

複数のデバイスを選択できます。

ステップ 3 **[追加（Add）]** または **[削除（Remove）]** アイコンをクリックして、パッチをインストールするための適切なスイッチを含めます。

選択したスイッチが右側の列に表示されます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 **[パッケージ（Packages）]** 列で **[パッケージの選択（Select Packages）]** をクリックします。

[SMU パッケージ ブラウザ（SMU Packages Browser）] ダイアログ ボックスが表示されます。

ステップ 6 **[SMU パッケージ ブラウザ（SMU Package Browser）]** ダイアログ ボックスで、**[ファイル サーバー（File Server）]** または **[ファイル システムの切り替え（Switch File System）]** からパッチ ファイルを選択できます。

[ファイル サーバー（File Server）] を選択した場合：

a) **[ファイル サーバーの選択（Select the file server）]** リストから、パッチが保存されている適切なファイル サーバーを選択します。

[リポジトリ（Repositories）] ウィンドウにリストされているサーバーがドロップダウン リストに表示されます。**[構成（Configure）] > [イメージ管理（Image Manageme）] > [リポジトリ（Repositori）]** を選択して、**[リポジトリ（Repositories）]** ウィンドウを表示します。

b) **[イメージの選択（Select Image）]** リストから、デバイスにインストールする必要がある適切なパッチを選択します。

デバイスにインストールするパッチ ファイルを複数選択できます。

Note パッチのインストールによってデバイスが再起動する場合は、パッチ ファイルを 1 つだけ選択します。

同じプラットフォームの他のすべての選択されたデバイスに同じパッチを使用するには、チェック ボックスをオンにします。

ファイル サーバーを選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

c) **[VRF]** ドロップダウン リストから仮想ルーティングと転送（VRF）の IP アドレスを選択します。

ドロップダウン リストの 2 つのオプションは、**管理**と**デフォルト**です。

チェックボックスをオンにして、選択した他のすべてのデバイスに同じ VRF を使用します。

d) **[OK]** をクリックしてパッチイメージを選択するか、**[キャンセル]** をクリックして SMU インストール ウィザードに戻ります。

[ファイル システムの切り替え（Switch File System）] :

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なパッチ ファイル イメージを選択します。

デバイスにインストールするパッチ ファイルを複数選択できます。

スイッチ ファイル システム（Switch File System）] を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックしてイメージを選択するか、**[選択のクリア（Clear Selections）]** をクリックしてすべてのチェック ボックスをオフにするか、**[キャンセル（Cancel）]** をクリックして **[SMU パッケージ ブラウザ（SMU Package Browser）]** ダイアログ ボックスに戻ります。

ステップ 7 **[完了（Finish）]** をクリックします。

確認ウィンドウが表示されます。[OK] をクリックします。

Note SMU を再ロードすると、SMU のインストールによりスイッチが再ロードされる場合があります。

[DCNM] > [インベントリ（Inventory）] > [スイッチ（Switches）] を選択すると、**[スイッチ（Switches）]** ウィンドウでスイッチにインストールされているパッチのリストを表示できます。

パッチのアンインストール

Cisco DCNM Web クライアントからデバイスのパッチをアンインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [パッチ [SMU]（Patch [SMU]）] > [インストール履歴（Installation History）]** を選択し、**[アンインストール（Uninstall）]** をクリックします。

[スイッチの選択（Select Switches）] ページが表示されます。検出された Cisco Nexus スイッチが表示されます。

ステップ 2 スイッチ名の左側にあるチェックボックスを選択します。

複数のイメージ デバイスを選択できます。

ステップ 3 **[追加（Add）]** または **[削除（Remove）]** アイコンをクリックして、パッチをインストールするための適切なスイッチを含めます。

選択されたスイッチが右の列に表示されます。

ステップ 4 [次へ（Next）] をクリックします。

[アクティブ パッケージ（Active Packages）] ページが表示されます。

ステップ 5 **[インストール済みパッケージ（Installed Packages）]** 列の下の **[パッケージの選択（Select Packages）]** をクリックします。

[インストールされたパッケージ（Packages Installed）] ウィンドウが表示され、スイッチにインストールされているパッチがリストされます。

ステップ 6 このデバイスからアンインストールするパッチを選択します。

デバイスに適用するパッチを複数選択できます。

Note パッチのアンインストールによってデバイスが再起動する場合は、パッチを 1 つだけ選択します。

ステップ 7 **[完了（Finish）]** をクリックして、パッチをデバイスからアンインストールします。

確認ウィンドウが表示されます。[OK] をクリックします。

一度に複数のパッチをアンインストールできます。

Note SMU が再ロードされた場合、SMU のアンインストールによりスイッチが再ロードされる場合があります。

パッチ インストール タスクの削除

Cisco DCNM Web UI からパッチ インストール タスクを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [パッチ [SMU（Patch [SMU]）]（）] > [インストール履歴（Installation History）]** を選択し、タスク ID チェックボックスをオンにします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 **[OK]** をクリックして、パッチ インストール タスクの削除を確認します。

スイッチのインストール済みのパッチ

ネットワーク内のすべてのスイッチにインストールされているパッチを表示できます。ビューを更新して、インストールされている最新のパッチを表示できます。

次の表では、**[構成（Configure）] > [画像管理（Image Management）] > [パッチ [SMU]（Patch [SMU]）] > [インストールされたパッチの切り替え（Switch Installed Patches）]** 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	スイッチの名前を示します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
プラットフォーム [英語]	Cisco Nexus スイッチング プラットフォームを指定します。
インストールされたパッチ	スイッチに現在インストールされているパッチを指定します。

表を更新するには、**[更新（Refresh）]**をクリックします。

パッケージ [RPM]

パッケージ [RPM] メニューには以下のサブメニューが含まれます。

パッケージのインストール [RPM]

パッケージ [RPM] 機能を使用すると、RPM パッケージをインストールできます。この機能は Cisco Nexus 9000 シリーズと 3000 シリーズ スイッチで利用可能です。

次のテーブルは、**[構成（Configure）] > [イメージ管理（Image Management）] > [パッケージ [RPM]（Package [RPM]）] > [インストール履歴（Installation History）]**に現れるフィールドを説明します。

フィールド	説明
タスク ID（Task Id）	タスクのシリアル番号を指定します。最新のタスクが上部に表示されます。 タスクは順番に実行されます。
スイッチ名	パッケージ ファイルがインストールされているスイッチの名前を指定します。
IPAddress	デバイスの IP アドレスを指定します。
タスク	パッケージがこのデバイスにインストールされているかアンインストールされているかを指定します。
パッケージ	パッケージ ファイルの名前を指定します。
ステータス（Status）	パッケージ ファイルのインストールまたはアンインストールのステータスを指定します。
完了時刻	インストールまたはアンインストール タスクが完了した時刻を指定します。
ステータスの説明	パッケージ ファイルのインストールまたはアンインストールのステータスを説明します。

この項の内容は、次のとおりです。

パッケージ [RPM] のインストール

Cisco DCNM Web クライアントを使用してデバイスにパッケージをインストールするには、次のタスクを実行します。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [パッケージ [RPM]（Package [RPM]）] > [インストール履歴（Installation History）]** を選択し、**[インストール（Install）]** をクリックします。

[スイッチの選択（Select Switches）] ページが表示されます。

ステップ 2 スイッチ名の左側にあるチェックボックスを選択します。

複数のデバイスを選択できます。

ステップ 3 **[追加（Add）]** または **[削除（Remove）]** をクリックして、パッケージをインストールするための適切なスイッチを含めます。

選択されたスイッチが右の列に表示されます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 **[パッケージ（Packages）]** 列の **[パッケージの選択（Select Packages）]**をクリックします。

[RPM パッケージ ブラウザ画面（RPM Package Browser）] が表示されます。

ステップ 6 **[ファイル サーバ（File Server）]**または**スイッチ ファイル システム（Switch File System）]**からパッケージ ファイルを選択します。

[ファイル サーバ（File Server）] を選択した場合：

a) **[ファイル サーバーの選択（Select the file server）]** リストから、パッケージが保存されている適切なファイル サーバを選択します。

[構成（Configure）] > [画像管理（Image Management）] > [リポジトリ（Repositories）] のサーバが、ドロップダウン リストに表示されます。

b) **[イメージの選択（Select Image）]** リストから、デバイスにインストールする必要がある適切なパッケージを選択します。

デバイスにインストールするパッケージ ファイルを複数選択できます。

[ファイル サーバ（File Server）] を選択すると、RPM 拡張子を持つファイルのみがリストされます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバを再起動します。デフォルトでは **true** に設定されています。

同じプラットフォームの他のすべての選択されたデバイスに同じパッケージを使用するには、チェックボックスをオンにします。

c) **[OK]** をクリックしてパッチ イメージを選択するか、**[キャンセル（Cancel）]** をクリックして RPM インストール ウィザードに戻ります。

[スイッチ ファイル システム（Switch File System）] :

a) **[画像の選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なパッケージ ファイル 画像を選択します。

デバイスにインストールするパッケージ ファイルを複数選択できます。

スイッチ ファイル システム（Switch File System）] を選択すると、RPM 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバを再起動します。デフォルトでは **true** に設定されています。

b) [OK] をクリックします。

ステップ 7 **[インストール タイプ（Installation Type）]** 列で、いずれかのインストール タイプを選択します。

- **[通常（Normal）]**—新規インストール
- **[アップグレード（Upgrade）]** — 既存の RPM のアップグレード
- **[ダウングレード（Downgrade）]** — 既存の RPM のダウングレード

ステップ 8 **[完了（Finish）]** をクリックします。

スイッチにインストールされているパッケージのリストは、**[ウェブ クライアント（Web Client）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** ページで表示できます。

Note Cisco DCNM リリース 10.1（2）を使用している場合で、リロード RPM をインストールする際は、スイッチのリロード後にスイッチで手動インストールコミットを実行します。

パッケージ [RPM] のアンインストール

Cisco DCNM Web UI からデバイスで RPM をアンインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [パッケージ [RPM]（Package [RPM]）] > [インストール履歴（Installation History）]** を選択し、**[アンインストール（Uninstall）]** をクリックします。

[スイッチの選択（Select Switches）] ウィンドウが表示されます。

ステップ 2 スイッチ名の左側にあるチェックボックスを選択します。

複数のスイッチを選択できます。

ステップ 3 **[追加（Add）]** または **[削除（Remove）]** アイコンをクリックして、パッケージをアンインストールするための適切なスイッチを含めます。

選択されたスイッチが右の列に表示されます。

ステップ 4 [次へ（Next）] をクリックします。

[現用系 パッケージ（Active Packages）] ページが表示されます。

ステップ 5 **[インストール済みパッケージ（Installed Packages）]** 列の下の **[パッケージの選択（Select Packages）]** をクリックします。

[インストールされたパッケージ（Packages Installed）] ウィンドウが表示され、スイッチにインストールされているパッケージがリストされます。

ステップ 6 **[完了（Finish）]** をクリックして、パッケージをデバイスからアンインストールします。

確認ウィンドウが表示されます。[OK] をクリックします。

一度に複数のパッケージをアンインストールできます。

Note

- Cisco DCNM リリース 10.1（2）を使用している場合、リロード RPM をアンインストールする場合、スイッチがリロードされたら手動でインストールコミットをスイッチで実行する必要があります。
- RPM がリロード RPM の場合、RPM のアンインストールによりスイッチがリロードされる場合があります。

パッケージ インストール タスクの削除

Cisco DCNM Web UI の履歴ビューからパッケージ インストール タスクを削除するには、以下の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理]（Image Management） > [パッケージ [RPM]（Package [RPM]）] > [インストール履歴（Installation History）]** を選択し、タスク ID チェック ボックスをオンにします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 **[OK]** をクリックして、タスクの削除を確認します。

インストール済みパッケージの切り替え

ネットワーク内のすべてのスイッチにインストールされている RPM パッケージを表示できます。ビューを更新して、インストールされている最新のパッケージを表示できます。

次の表では、**[構成（Configure）] > [イメージ管理（Image Management）] > [パッケージ [RPM]（Packages [RPM]）] > [インストール済みパッケージの切り替え（Switch Installed Packages）]** 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	スイッチの名前を示します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
プラットフォーム [英語]	Cisco Nexus スイッチ プラットフォームを指定します。
インストール済みパッケージ	スイッチに現在インストールされているパッケージとパッケージのタイプを指定します。インストールされるパッケージは、基本パッケージまたは非基本パッケージです。

表を更新するには、**[更新（Refresh）]**をクリックします。

メンテナンス モード [GIR]

メンテナンス モード [GIR] メニューには次のサブメニューが含まれます。

メンテナンス モード

メンテナンス モードでは、Graceful Insertion and Removal（GIR; グレースフル挿入および削除）を使用して、ネットワークからCisco Nexusスイッチを分離して、アップグレードまたはデバッグを実行できます。スイッチのメンテナンスが完了したら、スイッチを通常モードに戻すことができます。スイッチがメンテナンス モードの場合、すべてのプロトコルが正常に停止し、すべての物理ポートがシャットダウンされます。通常モードに復元すると、すべてのプロトコルおよびポートがイニシエートに戻ります。

デバイスのシステム モードを変更するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [イメージ管理（Image Management）] > [メンテナンス モード [GIR]（Maintenance Mode [GIR]）] > [メンテナンス モード（Maintenance Mode）]** を選択し、スイッチ名のチェックボックスをオンにします。

複数のスイッチを選択できます。

ステップ 2 **[モードの選択（Mode Selection）]** 列で、次のオプションのいずれかを選択します：

- シャットダウン
- 分離

Note モードを変更する前に、適切なオプションをクリックしてください。

ステップ 3 **[システム モードを変更（Change System Mode）]**をクリックします。

確認メッセージが表示されます。

ステップ 4 **[OK]** をクリックして、デバイスのメンテナンス モードを変更することを確認します。

稼働状況は、**[システムモード（System Mode）]**と**[メンテナンスステータス（Maintenance Status）]**で確認できます。

スイッチのメンテナンス履歴

Cisco DCNM から実行されたメンテナンス モードの変更の履歴を表示できます。

次の表では、**[構成（Configure）] > [画像管理（Image Management）] > [メンテナンス モード [GIR]（Maintenance Mode [GIR]）] > [スイッチのメンテナンス履歴（Switch Maintenance History）]** 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
タスク ID（Task Id）	タスクのシリアル番号を指定します。上部にリストされている最新のタスク。
スイッチ名	メンテナンス モードを変更したスイッチ名を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
ユーザ	メンテナンスを開始したユーザーの名前を指定します。
システムモード	システムのモードを指定します。
メンテナンスステータス	メンテナンスプロセスのモードを指定します。
ステータス（Status）	モード変更のステータスを指定します。
完了時刻	メンテナンス モードアクティビティが完了した時刻を指定します。

スイッチ名の横にあるラジオボタンをクリックして、アップグレード履歴を表示する必要があるスイッチを選択します。**[表示（View）]**をクリックして、選択したスイッチのアップグレード タスク履歴を表示します。

次の表では、**[構成（Configure）] > [画像管理（Image Management）] > [アップグレード [ISSU]（Upgrade [ISSU]）] > [スイッチ レベルの履歴（Switch Level History）] > [表示（View）] > [アップグレード タスクの履歴（Upgrade Tasks History）]** 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
オーナー（Owner）	アップグレードを開始した所有者を指定します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了）
キックスタート画像	スイッチのアップグレードに使用するキックスタート画像を指定します。
システムのイメージ（System Image）	スイッチのアップグレードに使用するシステム画像を指定します。

フィールド	説明
完了時刻	アップグレードが正常に完了した日時を指定します。

[画像と構成サーバー（Image and Configuration Servers）]

Cisco DCNM Web UI ホームページから **[画像と構成サーバー（Image and Configuration Servers）]** ウィンドウを表示するには、**[構成（Configure）] > [画像管理（Image Management）] > [リポジトリ（Repositories）]** を選択します。

[画像と構成サーバー（Image and Configuration Servers）] ウィンドウで、次の詳細を表示できます。

フィールド	説明
Name	アップロードするリポジトリの名前を指定します。
URL	リポジトリをアップロードしたパスを指定します。
ユーザ名	リモート サーバーのユーザー名を指定します。
最終更新日	最終変更のタイムスタンプを指定します。

イメージの追加または構成サーバ URL

Cisco DCNM Web UI から出し入れする画像またはリポジトリの構成 サーバ URLを追加するには、次の操作を行なってください。

Procedure

ステップ 1 **[画像および構成サーバ（Image and Configuration Servers）]** ウィンドウで、**[追加（Add）]** アイコンをクリックします。

[画像または構成サーバ URL の追加（Add Image or Configuration Server URL）] ウィンドウが表示されます。

ステップ 2 画像の名前を指定します。

ステップ 3 ラジオ ボタンをクリックし、プロトコルを選択します。

使用可能なプロトコルは、**SCP**、**FTP**、**SFTP**、**TFTP** です。POAP および画像管理に SCP プロトコルを使用します。

これらのプロトコルでは、IPv4 および IPv6 アドレスを使用できます。

ステップ 4 ホスト名または IP アドレスと、ファイルをダウンロードまたはアップロードするパスを入力します。

Note **SCP** または **SFTP** プロトコルを選択し、パスがルートまたは / ディレクトリの場合、画像または構成サーバの追加は失敗します。

ステップ 5 ユーザー名とパスワードを指定します。

ステップ 6 [OK] をクリックして保存します。

イメージの削除

Cisco DCNM Web UI から画像をリポジトリから削除するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [リポジトリ（Repositories）]** を選択します。

[画像および構成サーバー（Image and Configuration Servers） ウィンドウが表示されます。

ステップ 2 リストから既存の画像を選択し、**[画像の削除（Delete Image）]** アイコンをクリックします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックして、イメージを削除します。

画像もしくは構成 サーバー URLを編集

Cisco DCNM ウェブ UI からリポジトリへ画像もしくは構成 サーバー URLを編集するには、次の操作を行なってください。

Procedure

ステップ 1 **[イメージおよび構成サーバー（Image and Configuration Servers）]** ウィンドウで、リストから既存のイメージおよび構成サーバーを選択し、**[編集（Edit）]**をクリックします。

ステップ 2 **[イメージまたは構成サーバーの URL の編集（Edit Image or Configuration Server URL）]** ウィンドウで、必要なフィールドを編集します。

ステップ 3 保存するために **OK** をクリックもしくは、変更を破棄するために**[キャンセル（Cancel）]**をクリックします。

ファイルの参照

サーバーのコンテンツは、**[イメージ サーバーと構成サーバー（Image and Configuration Servers）]**ページで表示できます。

1. **[イメージと構成（Image and Configurations）]** ページで、**[サーバー名（Server Name）]** チェックボックスをオンにしてコンテンツを表示します。
2. **[ファイル ブラウザ（File Browser）]** をクリックして、このサーバーのコンテンツを表示します。

イメージのアップロード

Cisco DCNM Web UI からサーバーにさまざまなタイプの画像をアップロードするには、次の手順を実行します。

Note 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。で使用されます。

画像をアップロードするには、ユーザー ロールが **network-admin** または 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。

Procedure

ステップ 1 **[構成（Configure）] > [画像管理（Image Management）] > [リポジトリ（Repositories）]**を選択します。

[画像および構成サーバー（Image and Configuration Servers） ウィンドウが表示されます。

ステップ 2 **[画像のアップロード（Image Upload）]** をクリックします。

[アップロードするファイルを選択（Select File to Upload）] 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、**[アップロード（Upload）]**をクリックする。

ステップ 5 [OK] をクリックします。

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。

LAN テレメトリの正常性

DCNM 11.2（1）以降、DCNM のストリーミング ローカル エリア ネットワーク（LAN）テレメトリ プレビュー機能は廃止され、ネットワーク インサイト技術情報（NIR）アプリケーションに置き換えられました。NIR は、**[Web UI] > [アプリケーション（Applications）]**で Cisco DCNM アプリケーション フレームワークを使用して展開できます。ファブリックで NIR を有効にすると、Cisco DCNM Web UI の ウィンドウでステータスをモニタリングできます。

接続ステータスが **[切断（Disconnected）]** として表示されると、ポート構成はスイッチで適切に承認されない場合があります。スイッチ画像 7.0(3)I7(6) で、スイッチにすでに **nxapi** 構成があり、その後、DCNMによって管理されテレメトリがそのファブリックで有効になった場合、DCNM は **http port 80** 構成をプッシュすることで、一部 NXAPI コマンド（**show telemetry transport** および **show telemetry data collector details**など）をクエリして、テレメトリ接続統計情報をモニタできます。この場合、コマンドが適切に実行されてもスイッチは構成で **http port 80** を更新しません。このようなシナリオの場合、スイッチで次のコマンドを発行します。

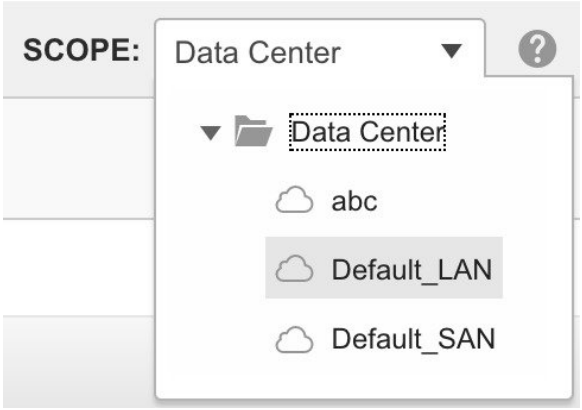
```
switch# configure
switch(config)# no feature nxapi
switch(config)# feature nxapi
switch(config)# http port 80
```

（注） TCAM や ACL TCAM 転送などの ICAM テレメトリ コマンドは、スイッチ画像 7.0(3)I7(5) および 7.0(3)I7(6) の Cisco Nexus C9504、C9508、および C9516 シリーズ プラットフォームではサポートされていません。

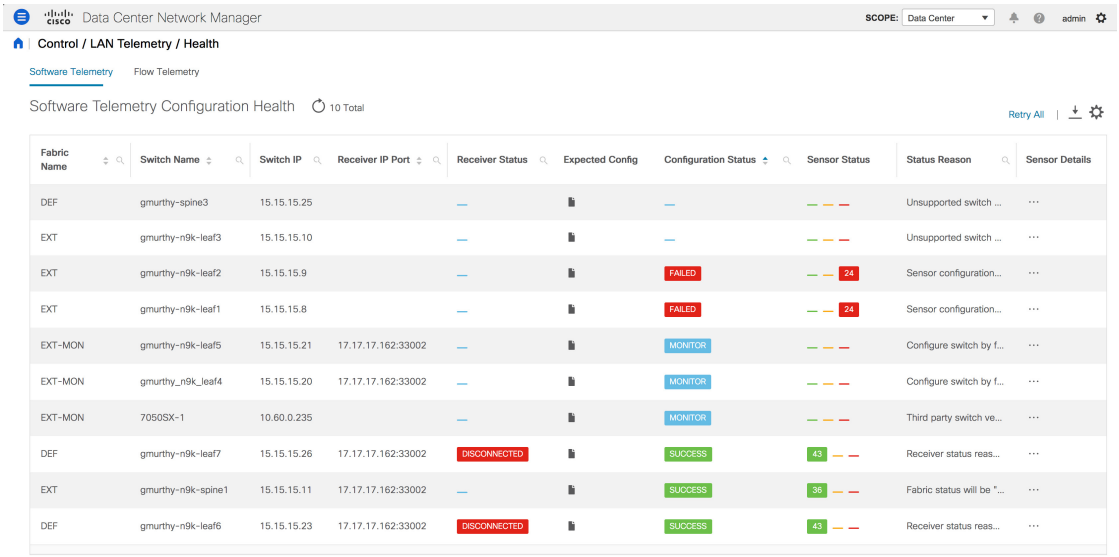
ローカル エリア ネットワーク（LAN）テレメトリには、次のトピックがあります。

ヘルス（Health）

Cisco DCNM を使用すると、ファブリックごとにソフトウェア テレメトリとフロー テレメトリの構成正常性属性をモニタするできます。属性は特定のファブリックまたは選択された**SCOPE** に基づいたすべてのファブリックに対して表示されます。**[Data Center 範囲（Data Center scope）]**には、デフォルトですべてのファブリックが表示されます。



ソフトウェアテレメトリ



次の表は、**[ローカル エリア ネットワーク（LAN）テレメトリ（LAN Telemetry）] > [正常性（Health）] > [ソフトウェア テレメトリ（Software Telemetry）]** ウィンドウに表示されるフィールドについて説明しています。

フィールド	説明
Fabric Name（ファブリック名）	ファブリック名を表示します。
スイッチ名	スイッチの名前が表示されます。
IPのスイッチ	スイッチの管理 IP アドレスを表示します。

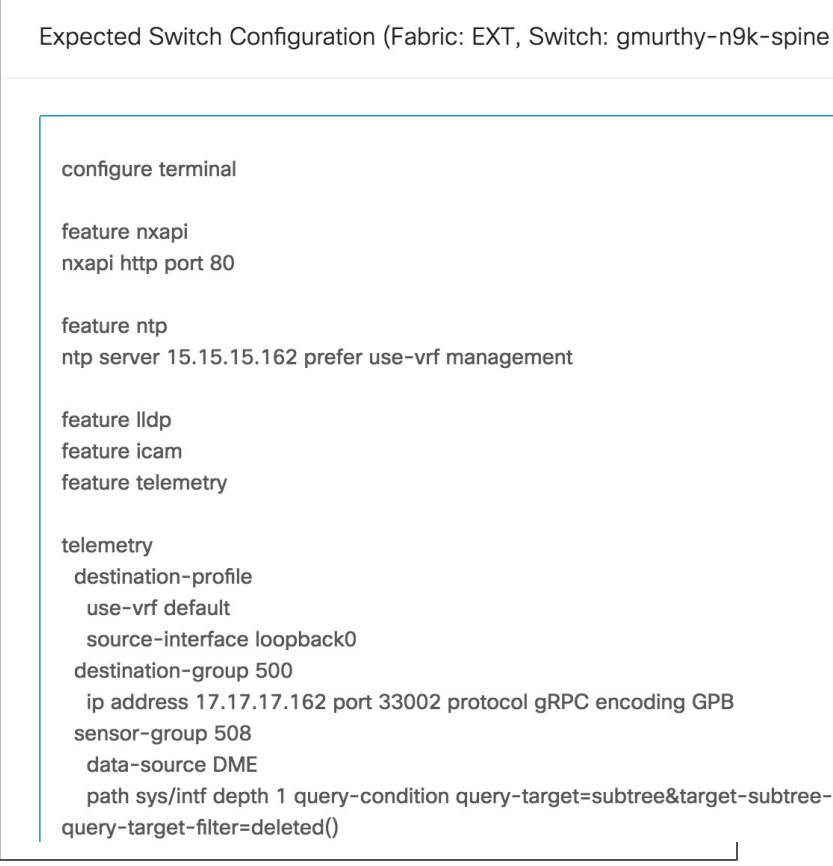
フィールド	説明
スイッチのシリアル	スイッチのシリアル番号を表示します。 デフォルトでは、この列は隠れています。**[設定（Settings）]** アイコンをクリックし、**[シリアルの切り替え（Switch Serial）]** チェック ボックスをオンにして、表示される列に追加します。
スイッチ モデル	スイッチのモデルを表示します。 デフォルトでは、この列は隠れています。**[設定（Settings）]** アイコンをクリックし、**[モデルの切り替え（Switch Model）]** チェック ボックスをオンにして、表示される列に追加します。
バージョン切り替え	スイッチ イメージのバージョンを表示する。 デフォルトでは、この列は隠れています。**[設定（Settings）]** アイコンをクリックし、**[バージョンの切り替え（Switch Version）]** チェック ボックスをオンにして、表示される列に追加します。
受信者 IP ポート	テレメトリ データを転送するためにスイッチに割り当てられた受信側 IP とポートを表示します。 割り当てられる IP とポートは、構成されたテレメトリ ネットワーク、アウトオブバンドまたはインバンド、および NIR アプリケーションで実行されている対応する受信者マイクロサービスに基づいています。

フィールド	説明

受信者ステータス	スイッチとNIRアプリケーションで実行されている受信機との間でテレメトリデータを転送するために使用される接続のステータスを表示します。
	
	テレメトリ マネージャは、5分ごとに接続ステータスについてスイッチをポーリングします。
	
	有効な値は次のとおりです。
	
	• **[接続済み（Connected）]**：テレメトリ マネージャーがスイッチからの受信者接続ステータスをポーリングできる場合、ステータスは**[接続済み（Connected）]**です。
	
	• **[切断（Disconnected）]**：ステータスが**[切断（Disconnected）]**の場合、その理由は**[ステータスの理由（Status Reason）]**列に表示されます。
	
	• **Null** ：DCNMのテレメトリ マネージャがスイッチからのレシーバ接続ステータスをポーリングしていない場合、またはその要求に対するスイッチからの応答を受信していない場合、ステータスは**Null**です。受信者のステータスが **Null** で、構成ステータスが**MONITOR**または**SUCCESS**の場合は、スイッチにログインしてnxapi構成を確認します。
	
	DCNMによって管理されるファブリックでテレメトリを有効にすると、テレメトリ マネージャは **httpport 80** 構成をプッシュします。スイッチにhttpport 80構成がない場合は、スイッチで次のコマンドを実行します。
	
	`switch# configure terminal`
	`switch(config)# no feature nxapi`
	`switch(config)# feature nxapi`
	`switch(config)# http port80`

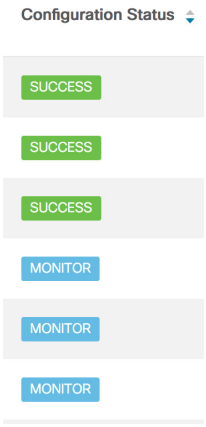
設定タイプ	スイッチによって報告された接続タイプ（例: gRPC）を表示します。この値は、スイッチからの受信者接続ステータス応答の一部として取得されます。デフォルトでは、この列は隠れています。設定ボタンから選択できます。

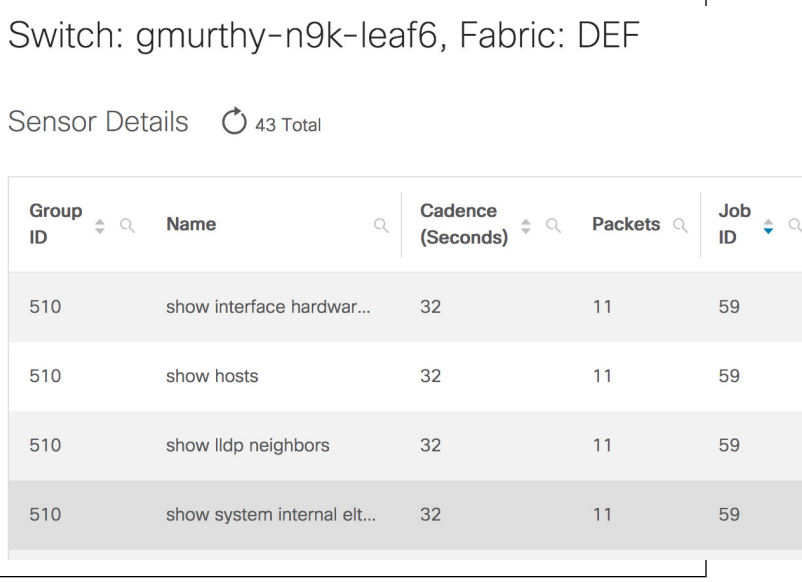
フィールド	説明
想定される構成	**[予想される構成（Expected Config）]** アイコンをクリックして、スイッチの予想される構成をダイアログボックスに表示します。エラーの場合、エラーの理由が出力に表示されます。



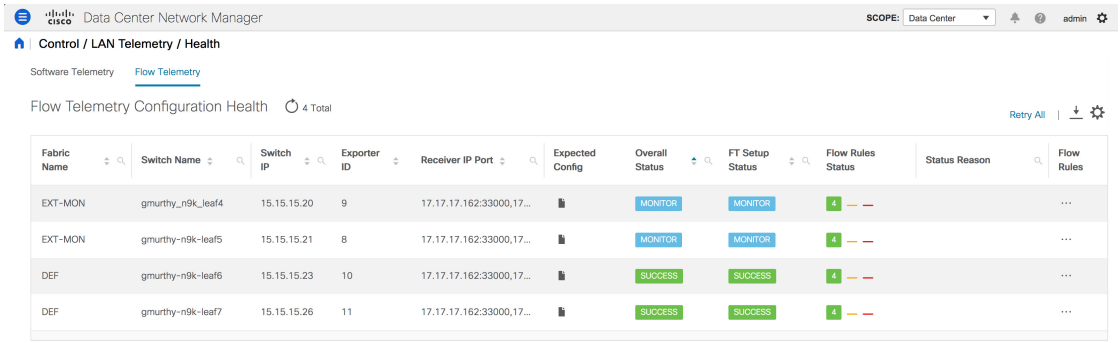
フィールド	説明
設定ステータス	

フィールド	説明
	テレメトリ構成スイッチのサマリー ステータスを表示します。 有効な値は次のとおりです。 • **MONITOR**：ファブリック内のスイッチがNIRアプリで**[モニタ対象（Monitored）]**として構成されたことを意味します。この場合、**[予想された構成（Expected Config）]**列に表示されているテレメトリ構成を使用して、これらのスイッチを手動で構成します。 • **PROCESSING**：ファブリックに属するスイッチがNIRアプリで**[管理対象（Managed）]**として構成されたことを意味します。この場合、テレメトリ マネージャーはスイッチを構成し、構成の進行中は **PROCESSING** と表示されます。 • **SUCCESS**：スイッチが正常に構成されたことを意味します。 • **PARTIAL SUCCESS**：一部のテレメトリ構成をスイッチにプッシュできなかったことを意味します。**[ステータスの理由（Status Reason）]** 列に失敗の理由が表示されます。 • **FAILED**：DCNM ジョブがスイッチの設定に機能不全になったを意味します。スイッチにプッシュされた構成とプッシュされなかった構成がある可能性があります。その場合、DCNM もジョブ全体を**[機能不全（Failed）]**としてマークします。**[ステータスの理由（Status Reason）]**列に失敗の理由が表示されます。 検索オプションを使用して特定のステータスに基づいてスイッチをフィルタ処理するか、ステータスに基づいてスイッチを並べ替えることができます。

フィールド	説明
	
センサーステータス	センサーの構成状態を色分けして表示します。センサー数は 3 つのカテゴリに分類されます。 • 緑色 (成功): 正常に構成されたセンサー パスの数 • 黄色 (保留中): 構成が保留されているセンサー パスの数 • 赤色（失敗）：構成できなかったセンサー パスの数
ステータス理由	テレメトリ構成ステータスおよび受信者接続ステータスまたはその他の情報の失敗理由を表示します。

フィールド	説明
センサーの詳細	次のセンサーの詳細を表示します。 • **[グループ ID（Group ID）]**：センサー パスが属するグループ ID • **[名前（Name）]**：スイッチに表示されるセンサー パス名：次に例を示します。 **show processes cpu** • **[Cadence（秒）（Cadence (Seconds)）]**：スイッチがそのセンサー パスをストリーミングするサンプル間隔 (秒単位)。例：値が 60 の場合、スイッチは 60 秒ごとにそのセンサー メトリクスをストリーミングします。 • **[パケット（Packets）]**：時間までに収集されるメトリクス サンプルの数を指定します。 • **[ジョブ ID（Job ID）]**：これは、スイッチのセンサー パスを構成するために使用された DCNM テレメトリ ジョブ 識別子 です。 • **ステータス**：ジョブのステータス。 • **[ステータスの理由（Status Reason）]**：ジョブのステータスの理由。ジョブが機能不全した場合は、そのジョブの機能不全の理由を示します。 

フローテレメトリ



[LAN テレメトリ（LAN Telemetry）] > [正常性（Health）] > [フロー テレメトリ（Flow Telemetry）] ウィンドウには、次のアイコンが表示されます。

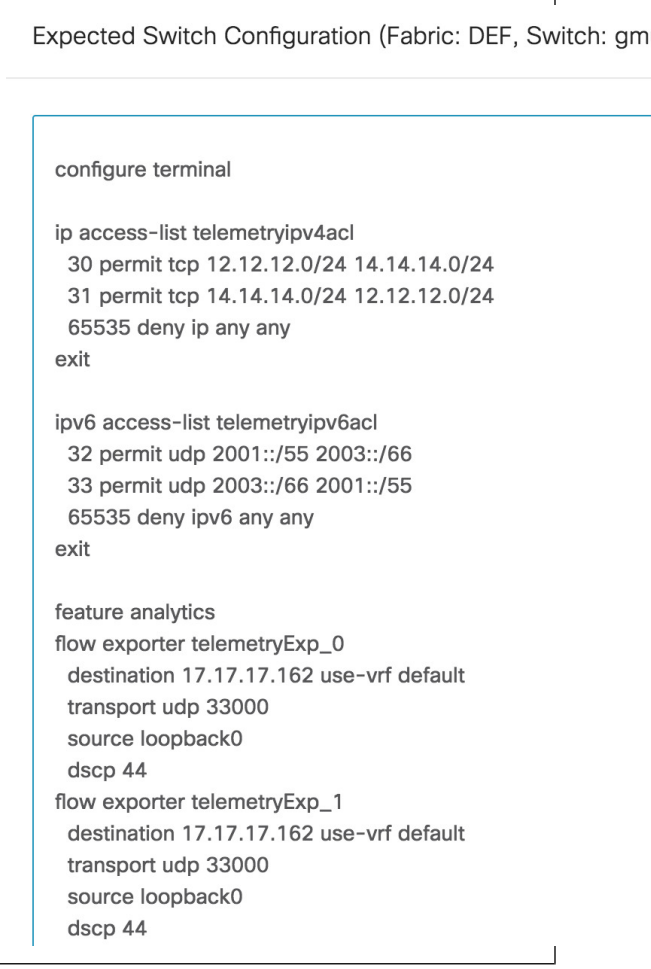
- **すべて再試行**：**[すべて再試行]**アイコンをクリックして、スイッチで機能不全になった構成を再試行します。ただし、このオプションは、サポートされていない構成の問題を自動的に修正しません。
- **エクスポート**：**[エクスポート]**アイコンをクリックして、データをスプレッドシートにダウンロードします。
- **設定**：**[設定]** アイコンをクリックして、表示する列を追加または削除します。

次の表では、**[LAN テレメトリ] > [ヘルス] > [フロー テレメトリ]** タブの列について説明します。

表 *21 : [*フロー テレメトリの健全性*]* タブのフィールドと説明

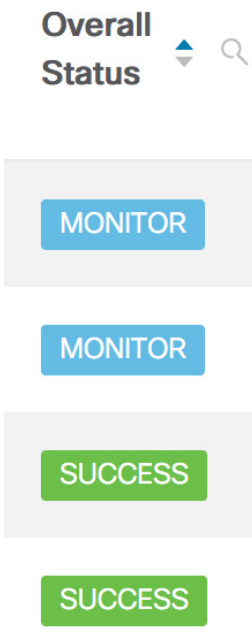
フィールド	説明
Fabric Name（ファブリック名）	ファブリックの名前を表示します。
スイッチ名	スイッチの名前が示されます。
IPのスイッチ	スイッチの管理 IP アドレスを表示します。
スイッチのシリアル	スイッチのシリアル番号を表示します。デフォルトでは、この列は隠れています。[設定] ボタンをクリックすることで、選択できます。
スイッチ モデル	スイッチのモデルを表示します。デフォルトでは、この列は隠れています。[設定] ボタンをクリックすることで、選択できます。
バージョン切り替え	スイッチ イメージのバージョンを表示する。デフォルトでは、この列は隠れています。[設定]ボタンをクリックすることで、選択できます。

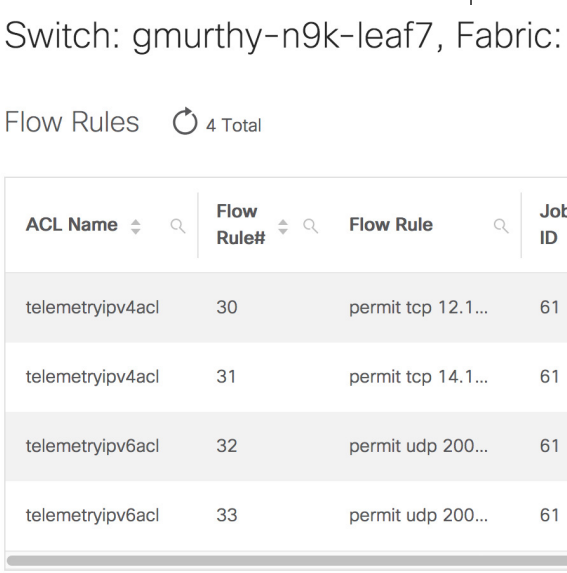
フィールド	説明
エクスポータ ID	フロー分析構成の一部としてスイッチに構成されているエクスポータ ID を表示します。
受信者 IP ポート	フローテレメトリ データを転送するためにスイッチに割り当てられた受信側 IP アドレスとポートのコンマ区切りリストを表示します。割り当てられた IP アドレスとポートは、NIR アプリケーションで実行され、帯域内ネットワークでリッスンしている、対応する受信側マイクロサービスのものになります。
予想される構成	クリックすると、ポップアップ ウィンドウにスイッチの予想される構成が表示されます。エラーの場合、エラーの理由が出力に表示されます。



フィールド	説明
全体のステータス	

フィールド	説明
	フローテレメトリ構成には、フローテレメトリ セットアップとフローACL構成の2つのコンポーネントが含まれます。全体的なステータス列には、これら両方のステータスの概要が表示されます。次のステータスが表示されます。 **モニタリング（MONITOR）**は、ファブリック内のスイッチがNIRアプリで「モニタリング対象」として構成されたことを意味します。この場合、[予想される構成（Expected Config）]列に表示されているテレメトリ構成を使用して、これらのスイッチを手動で構成することはあなたの責任です。 **処理中（PROCESSING）**：これは、ファブリックに属するスイッチがNIRアプリで「管理対象」として構成されたことを意味します。この場合、テレメトリ マネージャはスイッチを構成し、構成の進行中は「処理中（PROCESSING）」と表示されます。 **成功（SUCCESS）**：これは、スイッチが正常に構成されたことを意味します。 **一部成功（PARTIAL SUCCESS）**：一部のテレメトリ構成をスイッチにプッシュできなかったことを意味します。[ステータスの理由]列に失敗の理由が表示されます。 **機能不全（FAILED）**：これは、DCNMジョブがスイッチの構成が機能不全になったことを示します。スイッチにプッシュされた構成とプッシュされなかった構成がある可能性があります。その場合、DCNMもジョブ全体を失敗としてマークします。[ステータスの理由（Status Reason）]列に失敗の理由が表示されます。 検索オプションを使用して、特定のステータスに基づいてスイッチをフィルタリングできます(または、ステータスに基づいてスイッチをソートできます)。

フィールド	説明
	
FT 設定ステータス	フローテレメトリのセットアップ ステータスを表示します。これが **Failed（機能不全）** と表示されている場合は、スイッチでフロー分析を正しく有効にできなかったため、スイッチからフロー データをエクスポートできないことを示しています。
フロー ルール ステータス (または) フロー ACL ステータス	フロー ACL 構成ステータスを色分けされた形式で表示します。 フロー ルールのステータス カウントは、3 つのカテゴリに分類されます。 • 緑（成功）:正常に構成されたフロー ルール（ACE）の数。 • 黄色（保留中）:構成が保留されているフロー ルール（ACE）の数。 • 赤（失敗）:構成できなかったフロー ルール（ACE）の数。
ステータス理由	フロー テレメトリ構成（または）の他の情報の失敗理由を表示します。

フィールド	説明
フロールール	次のフロー ルールの詳細を表示します。 • **ACL 名**：スイッチに設定されているアクセス リストの名前。IPv4 の場合は telemetryipv4acl、IPv6 の場合は telemetryipv6acl の 2 つの ACL のみが作成されます。 • **Flow Rule#**：これは、特定の ACL 内で設定された ACE ルール番号です。 • **フロー ルール**：これは、プロトコル、送信元 IP、ソース ポート、宛先 IP、エクスポートする必要がある宛先ポートなどのフローの詳細を示す ACE ルールです。 • **ジョブ ID**：これは、スイッチでフロールールを構成するために使用された DCNM テレメトリ ジョブ ID です。 • **ステータス**：ジョブのステータス。 • **理由**：ジョブのステータス理由。ジョブが機能不全の場合、そのジョブの機能不全の理由が表示されます。成功したら、Lan Fabric 展開の場合、コンプライアンスと展開が成功したことを示す可能性があります。 

（注） MONITOR モードの場合、https:// で利用可能な次の API を使用して、スイッチでフローテレメトリを構成できます。<dcnm-ip> /api-docs: /telemetry/switches/{serialNumber}/flow-analytics-config -> ここで、serialNumber は文字列としてのスイッチのシリアル番号です。

正常性テーブルのデータは、70秒ごとに自動的に更新されます。[更新]アイコンをクリックすると、手動で更新できます。

SAN

SAN メニューには次のサブメニューが含まれます。

VSAN

Cisco DCNM リリース 11 以降、Cisco DCNM から Virtual SAN（VSAN）を構成および管理できます。メニュー バーから **[構成（Configure）] > [SAN] > [VSAN]** 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 範囲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 ファミリ 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 DCNM は、一時停止された VSAN を検出せず、表示もしません。

（注） DCNM 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。

選択した VSAN の範囲に関連付けられている情報が右側のパネルに表示されます。VSAN がセグメント化されている場合、セグメント化された個々の VSAN はそれぞれ VSAN の範囲です。選択したすべての VSAN の範囲について、タブに情報を表示できます。

- [スイッチ] タブ
- [ISLs] タブ
- [ホストポート] タブ

- [ストレージ（Storage）] タブ
- [属性（Attributes）] タブ
- [ドメイン ID] タブ
- [VSAN メンバーシップ] タブ

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 （262 ページ）」を参照してください。

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。

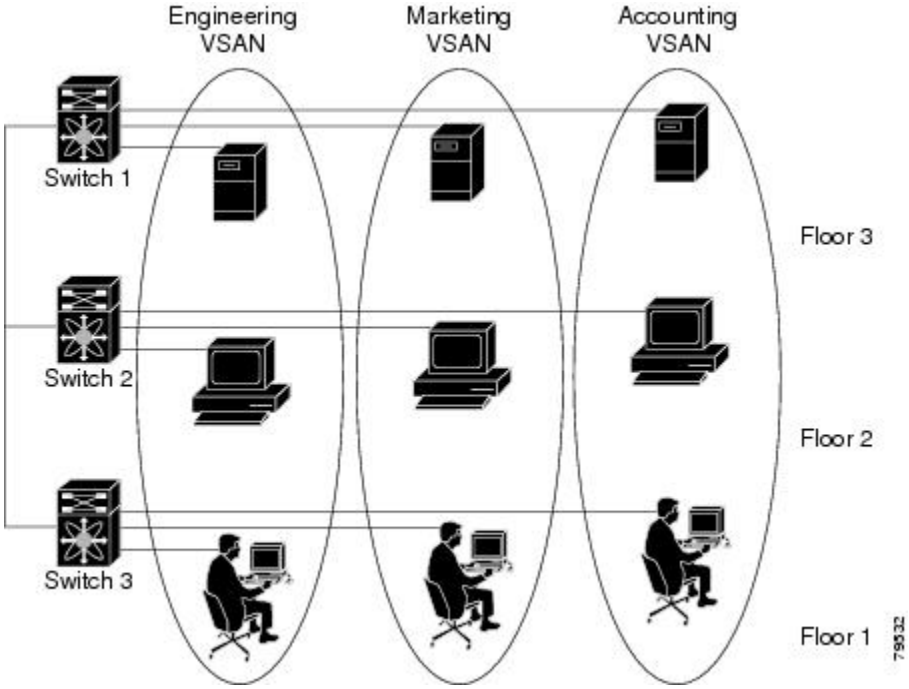
相互運用性により、複数ベンダー製品間の相互接続が可能になっています。ファイバチャネル標準規格では、ベンダーに対して共通の外部ファイバ チャネル インターフェイスを使用することを推奨しています。最大 8 つの VSAN で FICON をイネーブルできます。

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。

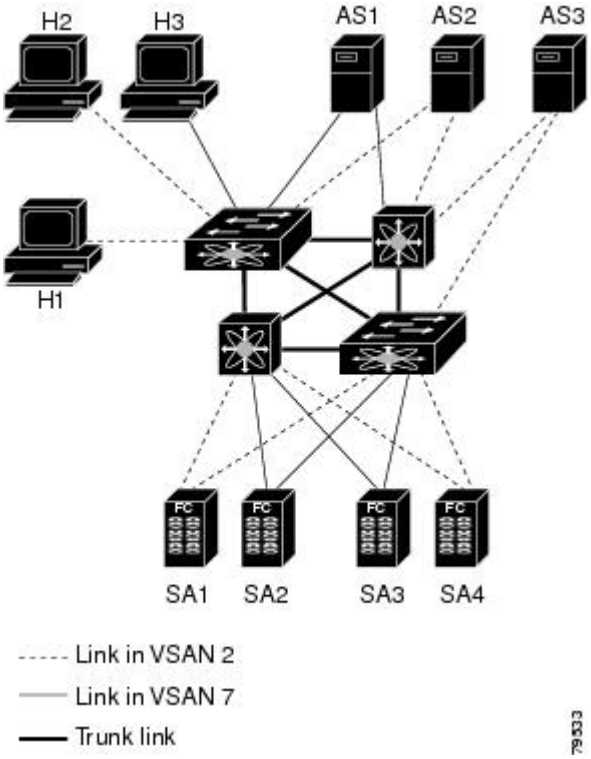
図 *1 :* 論理 *VSAN* の区分け



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 *2 : 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 ファミリ 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。

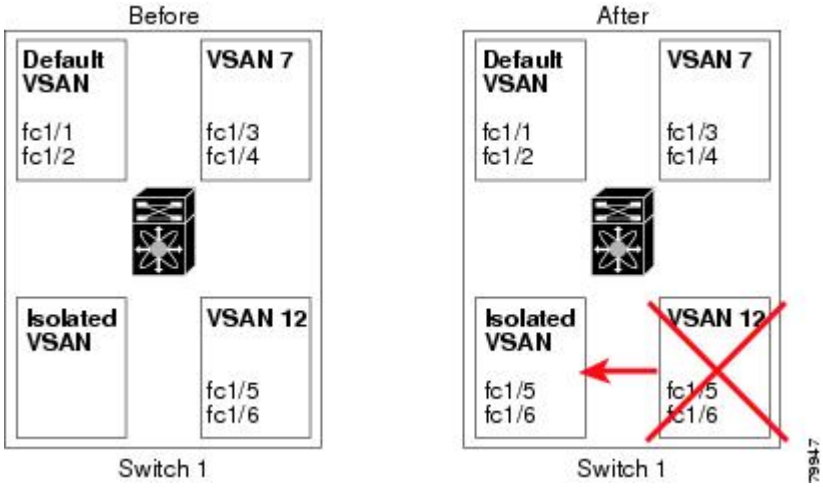
最大 256 の VSAN を 1 つのスイッチに設定できます。これらの VSAN の 1 つがデフォルト VSAN（VSAN 1）、もう 1 つが独立 VSAN（VSAN 4094）です。ユーザー指定の VSAN ID 範囲は 2 ～4093 です。

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 *3 : VSAN* ポート メンバーシップの詳細 – *79947.ps*



- 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 DCNM 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 DCNM 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。

リリース 11 以降、管理対象ファブリック内の複数のスイッチで VSAN を簡単に作成できるウィザードを使用して VSAN を構成できます。**[構成（Configure）] > [SAN] > [VSAN]** 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、**[VSAN ウィザードの作成（Create VSAN Wizard）]** 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。

（注） 検出ユーザーと異なる場合は、スイッチ資格情報を提供するようにしてください。SAN 資格情報を提供するには、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 資格情報（SAN Credentials）]** に移動します。

Cisco DCNM 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 の作成ウィザード初期画面で、**[次へ（Next）]**をクリックします。

[VSAN 識別子と名前を選択（Select VSAN ID and Name）] ウィンドウが表示されます。

ステップ 2 VSAN 識別子と名前を選択ウィンドウで、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) 名前フィールドに、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クリックして、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 3 スイッチの選択画面で、スイッチ名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 4 [VSAN 属性の構成（Config 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 DCNM で管理されないため、Cisco DCNM には表示されません。

a) ロードバランシングで、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。

- srcIdDestId:：送信元 ID（S_ID）と接続先 ID（D_ID）のみに基づいています。
- srcIdDestIdOxId：S_ID および D_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。OX_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） srcId/DestId/OxId は非 FICON VSAN のデフォルトであり、FICON VSAN では使用できません。srcId/DestId は FICON VSAN のデフォルトです。

b) [InterOp] フィールドで、ドロップダウン リストから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。

- 0：相互運用性が無効であることを意味します。
- 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。
- 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。
- 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。
- 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) 管理状態フィールドで、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） DCNM 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）] フィールドのチェックボックスをオンにします。

このチェック ボックスをオンにすると、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）] フィールドの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 5 [VSAN ドメインの構成（Configure VSAN Domain）] 画面で、FICON VSAN の静的ドメイン ID を設定します。

a) [静的ドメイン識別子 を使用する（Select the Use Static Domain IDs）] フィールドを選択して、VSAN 内のスイッチのドメイン ID を構成します。

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識別子を適用（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 6 [構成ポート VSAN メンバーシップ（Config Port VSAN 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 のメンバーとして構成します。

（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 7 [概要（Summary）] 画面で、VSAN が正しく構成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。

[キャンセル（Cancel）] をクリックしてこの構成を破棄します。

[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 DCNM 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 **[構成（Configure）] > [SAN] > [VSAN]** を選択します。

VSAN ウィンドウが表示されます。

ステップ 2 [ファブリック（Fabric）] 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 範囲ツリーが VSAN 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、削除する VSAN を選択します。

（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 の削除（Delete VSAN）]** 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。

ステップ 5 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。

[削除（Delete）] 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 6 削除を確認する場合は、**[はい（Yes）]** をクリックします。VSAN を削除しないでダイアログ ボックスを閉じる場合は、**[いいえ（No）]** をクリックします。

（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

[Cisco Web UI] > [SAN] > [VSAN] に表示されているすべてのタブのフィールドと説明は、以下の表で説明されています。

[スイッチ] 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 *22 : [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。Switch Summary のフィールドの説明については、スイッチのインベントリ情報の表示 （51 ページ） を参照してください。 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。
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。
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。
リフレッシュ	更新アイコンをクリックしてエントリを更新します。

[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。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。選択されたスイッチの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。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、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 *23 : 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。

フィールド	説明
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。
アイコン	
Total	合計の隣の番号は、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。

[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 *24 : [*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。
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。
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。
リフレッシュ	更新アイコンをクリックしてエントリを更新します。

[ストレージ（Storage）] 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 *25 : [*ストレージ*]* 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。
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。
リフレッシュ	更新アイコンをクリックしてエントリを更新します。

[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 *26 : [*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。 • ロード バランシング • 相互運用性 • InorderDelivery 属性を変更したら、**[適用（Apply）]** 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。
Name	VSAN の名前を表示します。

フィールド	説明
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 が構成され、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。 • **[一時停止（Suspended）]**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 DCNM 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。
LoadBalancing	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。 • 標準 • 相互運用性 - 1 • 相互運用性 - 2 • 相互運用性 - 3
InorderDelivery	デバイスの InOrderDelivery 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。
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。

[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 *27 : [*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 *28 : [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	[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（Miya#5341）、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

フィールド	説明
インターフェイス	VSAN の FC ポート
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。

SAN 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。

（注） web GUI/SAN クライアントのゾーニングにデバイス 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ニングを構成できます。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、**[構成（Configure）] > [SAN] > [ゾーニング（Zoning）]** タブの Cisco DCNM に現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
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、SAN ゾーニングを設定または表示するファブリックを選択できます。
VSAN	[VSAN] ドロップダウンリストから、通常のゾーニングを構成する VSAN を選択できます。
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。
変更の確定	すべてのスイッチに対してゾーニング構成の変更を確定します。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。
配信	ゾーニング構成をすべてのスイッチに配布します。このフィールドは、ゾーンが基本モードの場合にのみ適用されます。

フィールド	説明
すべてをエクスポート	ゾーニング構成を .csv ファイルにエクスポートして、ローカル ディレクトリに保存できます。
ゾーンセット	選択したファブリック、VSAN、およびスイッチに構成されているすべてのゾーン セットを一覧表示します。
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。
ゾーンメンバ	選択したゾーンに存在するメンバーを一覧表示します。
追加可能	ゾーンに追加できるデバイスを一覧表示します。
サーバー キャッシュを消去	Cisco DCNM サーバー上のキャッシュをクリアします。
保留中の変更の破棄	保留中の変更の破棄を実行中です。

この項の内容は、次のとおりです。

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。

Procedure

ステップ 1 Cisco DCNM Web UI からゾーンセットを作成するには、**[構成（Configure）] > [SAN ゾーン分割（SAN Zoning）] > [ゾーンセット（Zonesets）]** を選択し、**[ゾーンセットの作成（Create Zoneset）]** アイコンをクリックします。

[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、**[作成（Create）]** 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 ゾーンのラジオボタンを選択し、**ゾーンセットのクローン処理\コピー（Clone\Copy Zoneset）** アイコンをクリックして、ゾーンセットをクローン処理またはコピーします。

[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 **[アクション（Action）]** ラジオ 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、**[前に付加（Prepend）]** または **[追加（Append）]** 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。
- **[OK]** をクリックして、ゾーンセットをクローン処理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 ラジオ ボタンを選択してゾーンセット アイコンを削除をクリックします。

確認ウィンドウが表示されます。**[はい（Yes）]** をクリックして、ゾーンセットを削除します。

ステップ 5 ゾーン名を編集するには、ゾーン オプション ボタンを選択し、**[ゾーンセットの名前変更（Rename Zoneset）]** アイコンをクリックします。

[名前（Name）] フィールドに、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 ゾーンセットをアクティブにするには、ゾーンセット ラジオ ボタンを選択して**[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。

ステップ 7 ゾーンセットを非アクティブにするには、ゾーンセット ラジオ ボタンを選択して**[非アクティブ化（Deactivate）]**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。

ゾーン

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。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、または編集できます。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。

Note ゾーンを変更する必要がある **[ゾーンセット（Zoneset）]** を選択します。

ゾーンセット エリアで **[ゾーンセット（Zoneset）]** ラジオ ボタンを選択します。選択したゾーンセットで構成されているゾーンとスイッチのゾーンが表示されます。ゾーンの一部であるゾーンには、緑色のチェック マークが付いています。

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
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。
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。
スマート ゾーン	ゾーンがスマート ゾーンかどうかを指定します。 ゾーンがスマート ゾーンの場合、**true** を表示します。それ以外の場合は、**false** を表示します。 **[スマート ゾーン（Smart Zone）]** ドロップダウン リストから **[true]** または **[false]** を選択してこのフィールドを検索できます。このフィールドは、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表示されます。

Procedure

ステップ 1 ゾーンを作成するには、**[構成（Configure）] > [SAN] > [ゾーニング（Zoning）] > [ゾーン（Zone）]** を選択し、**[作成（Create）]** アイコンをクリックします。

a) [ゾーンの作成（Create Zone）] ウィンドウで、[ゾーン（Zone）] に有効な名前を入力し、**[作成（Create）]** をクリックします。

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 2 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 3 ゾーンをゾーンセットに追加するには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、ゾーン セットの一部ではないゾーンを選択します。**[ゾーンの追加（Add Zone）]** アイコンをクリックします。[ゾーンセット（Zoneset）] に追加するゾーンを複数選択できます。

ゾーンが選択された [ゾーンセット（Zoneset）] に追加されます。ゾーン名の横に緑色のチェックマークが表示され、ゾーンがゾーンセットに追加されたことを示します。

ステップ 4 ゾーン セットからゾーンを削除するには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** チェックボックスをオンにします。**[ゾーンの削除（Remove Zone）]** アイコンをクリックします。ゾーンセットから削除するゾーンを複数選択できます。

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 5 ゾーンを削除するには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** チェックボックスをオンにします。**[ゾーンの削除（Delete Zone）]** アイコンをクリックします。

確認ウィンドウが表示されます。

[はい（Yes）] をクリックして、選択したゾーンを削除します。

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。

ステップ 6 ゾーン名を編集するには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** ラジオ ボタンを選択します。**[ゾーンの名前変更（Rename Zone）]** アイコンをクリックします。

[名前（Name）] フィールドで、ゾーンに新しい名前を入力します。

[Rename] をクリックします。

ステップ 7 スマート ゾーンを有効にするには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** ラジオ ボタンを選択します。**[スマート ゾーンを有効にする（Enable Smart Zone）]** アイコンをクリックします。

[スマート ゾーン（Smart Zone）] 列の下には、True と表示されます。

ステップ 8 スマート ゾーンを無効にするには、**[構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン（Zones）]** を選択し、**[ゾーン（Zone）]** ラジオ ボタンを選択します。**[スマート ゾーンを無効にする（Disable Smart Zone）]** アイコンをクリックします。

[スマート ゾーン（Smart Zone）] 列の下には、false と表示されます。

ゾーン メンバー

選択したゾーンセットとゾーンに基づいて、[ゾーン メンバー（Zone 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。ゾーンセットのメンバーを作成または削除できます。

ゾーン 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
ゾーン	このメンバーが存在するゾーンを表示します。 このフィールドでゾーン名で検索できます。
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。
デバイスタイプ	スマート ゾーニングのデバイス タイプを表示します。 該当する値は、**ホスト**、**ストレージ**、または **両方**です。 このフィールドを検索するには、**[デバイス タイプ（Device Type）]** ドロップダウン リストから **[ホスト（Host）]**、**[ストレージ（Storage）]**、または **[両方（Both）]** を選択します。このフィールドは、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表示されます。
Name	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。

フィールド	説明
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイスを指定します。 スイッチ インターフェイスを指定して検索できます。
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。
WWN	スイッチの WWN を指定します。 スイッチの WWN を指定して検索できます。

Procedure

ステップ 1 ゾーン メンバーを作成するには、**[Cisco DCNM Web Client] > [構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン メンバー（Zone Members）]** から、[作成（Create）] アイコンをクリックします。

a) **[メンバーの作成と追加（Create and Add Member）]** ウィンドウで、ゾーン メンバーの WWN 名または [デバイス エイリアス（Device Alias）] を入力します。

Note デバイス エイリアス ゾーンにはオフライン メンバーのみを追加できます。

b) **[作成して追加（Create and Add）]** をクリックします。

作成と追加機能では、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も利用できます。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、**[Cisco DCNM Web Client] > [構成（Configure）] > [SAN ゾーニング（SAN Zoning）] > [ゾーン メンバー（Zone Members）]** から、**[ゾーン メンバー（Zone Member）]** チェックボックスをオンにします。**[メンバーを削除（Remove Member）]** をクリックします。

削除のために、一度に複数のゾーン メンバーを削除できます。

追加可能

[追加可能（Available to Add）] 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
タイプ	スマートゾーニングデバイスタイプを表示します。 適用できる値は**[ホスト（Host）]**と**[ストレージ（Storage）]**です。 **[ホスト（Host）]**、**[ストレージ（Storage）]**もしくは、**[タイプ（Type）]**をドロップダウンリストから選択することによってこのフィールドを検索する事ができます。
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。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチインターフェイスを指定します。 スイッチ インターフェイスを指定して検索できます。
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。
WWN	スイッチの WWN を指定します。 スイッチの WWN を指定して検索できます。

Cisco DCNM Web UI から検出されたデバイスを 1 つ以上のゾーンに追加するには 、以下の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [SAN] > [ゾーン分割（Zoning）] > [追加可能（Available to Add）]** を選択します。

ステップ 2 **[エリア別のゾーン（Zone by area）]**で、ポートまたはデバイスのエイリアスラジオ ボタンを選択します。

[エリア別のゾーン（Zone by area）] 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。

追加できるエンド ポートまたはデバイスのリストを示すウィンドウが表示されます。

[Zone by：**エンドポート（Zone By: End Port）]** 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。**[Zone By**：**デバイスのエイリアス（Zone By: Device Alias）]** を選択し

た場合、デバイスはデバイスエイリアスによってゾーンに追加されます。選択したエリア別のゾーンオプションに基づいて、デバイスが表示されます。

ステップ 3 ゾーンに追加するデバイスを選択します。

ステップ 4 **[追加（Add）]** をクリックして、選択したデバイスをゾーンに追加します。

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。

IVR ゾーニング

Cisco DCNM リリース 11.0（1) から、IVR ゾーン分割機能がサポートされます。IVR ゾーン分割を使用して、Web クライアントで IVR ゾーンを作成、編集、コピー、または削除できます。

[IVR ゾーニング（IVR Zoning）] ページは、Cisco DCNM の **[構成（Configure）]** > **[SAN]** > **[IVR ゾーン分割（IVR Zoning）]** メニュー項目から起動します。IVR ゾーン分割 ページを起動すると、次のフィールドとセクションが表示されます。

- ファブリック
- 地域ID
- スイッチ
- 変更の確定
- すべてをエクスポート
- サーバーキャッシュを消去
- 保留中の変更の破棄
- ゾーンセット
- ゾーンメンバ
- ゾーン
- 追加可能

次の表では、**[構成（Configure）]** > **[SAN]** > **[IVR ゾーン分割（IVR Zoning）]** タブの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
ファブリック	ファブリック ドロップダウン リストから、IVR ゾーン分割を構成または表示するファブリックを選択できます。リージョン識別子とスイッチのオプションを表示するには、ファブリックを選択する必要があります。

フィールド	説明
地域ID	リージョン識別子ドロップダウンリストから、スイッチのリージョンを選択できます。
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。ゾーンシード スイッチはデフォルトで選択されています。
変更の確定	IVR ゾーン分割構成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。
すべてをエクスポート	IVR ゾーン分割構成を .csv ファイルにエクスポートして、ローカル ディレクトリに保存できます。
サーバーキャッシュを消去	Cisco DCNM サーバで検出されたゾーン分割キャッシュをクリアします。
保留中の変更の破棄	保留中の変更の破棄を実行中です。

ゾーン セットを表示するには、目的のファブリック、リージョン 識別子、およびスイッチを選択する必要があります。これは、ファブリック、VSAN、およびスイッチを必要とする通常のゾーン分割とは異なります。

スイッチが選択されると 3 つのチェックが行われ、次の警告の 1 つ以上を含む警告ダイアログが表示される場合があります。

- IVR Cisco ファブリック サービスが有効になっていることを確認します。
- NAT と自動トポロジが有効になっていることを確認します。
- 既存の IVR ゾーン マージ障害があるかどうかを確認します。

IVR Cisco Fabric Services 機能が有効になっていない場合、**[アクティブ化（Activate）]**、**[非アクティブ化（Deactivate）]**、**[コミット変更（Commit Changes）]**、および **[保留中の変更の破棄（Discard Pending Changes）]** はブロックされます。IVR NAT および IVR 自動トポロジが有効になっていない場合、それらを有効にするようWarning（注意）が表示されます。

この項の内容は、次のとおりです。

ゾーンセット

選択したファブリック、リージョン、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、コピーまたはクローン、削除、名前変更、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、**[Cisco DCNM Web Client]** > **[構成（Configure）]** > **[SAN]** > **[IVR ゾーニング（IVR Zoning）]** > **[ゾーンセット（Zonesets）]** 領域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
ゾーンセットの作成	ゾーンセットを作成します。
ゾーンセットのコピー/複製	• コピー：ゾーンセットを作成し、元のゾーンセット内のゾーンのコピーを作成します。コピーされた名前は、指定された文字列を先頭または末尾に付加した既存の名前です。 • クローン—元のゾーンセットと同じゾーンを構成する新しい名前のゾーンセットのみを作成します。
ゾーンセットの削除	選択したゾーンセットを削除します。
ゾーンセットの名前を変更	選択したゾーンセットの名前を変更します。
ゾーンセット	選択したファブリック、リージョン 識別子、およびスイッチに構成されているすべてのゾーンセットを一覧表示します。
ステータス（Status）	ゾーン セットがアクティブかどうかを表示します。
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。

Procedure

ステップ 1 ゾーンセットを作成するには、**[構成（Configure）]** > **[SAN]** > **[IVR ゾーニング（IVR Zoning）]** > **[ゾーンセット（Zonesets）]** を選択します。**[ゾーンセットの作成（Create Zoneset）]** アイコンをクリックします。

a) ゾーンセットに有効な名前をゾーンセット作成ウィンドウの中で入力します。
b) [作成（Create）] 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 2 ゾーンセットをクローンまたはコピーするには、**[構成（Configure）]** > **[SAN]** > **[IVR ゾーニング（IVR Zoning）]** > **[ゾーンセット（Zonesets）]** を選択します。コピーまたは複製するゾーンセットのラジオボタンを選択します。**[クローン\コピー ゾーンセット（Clone\Copy Zoneset）]** アイコンをクリックします。

[クローン\コピー ゾーンセット（Clone\Copy Zoneset）] ウィンドウには 2 つのオプションが表示されます。

a) 適切なアクション ラジオ ボタンをクリックします。

次のいずれかを選択できます。

- **[コピー（Copy）]**—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、**[前に付加（Prepend）]** または **[追加（Append）]** オプション ボタンを選択します。
- **[クローン（Clone）]** — 名前フィールドに、新しいゾーンセットの有効な名前を入力します。

b) **[OK]** をクリックして、ゾーンセットをクローン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 3 ゾーンセットを削除するには、**[構成（Configure）] > [SAN] > [IVR ゾーニング（IVR Zoning）] > [ゾーンセット（Zonesets）]** を選択します。**[ゾーンセット（Zoneset）]** ラジオ ボタンを選択します。**[ゾーンセットの削除（Delete Zoneset）]** アイコンをクリックします。

確認ウィンドウが表示されます。

[はい（Yes）] をクリックして、ゾーンセットを削除します。

ステップ 4 ゾーンセット名の名前を変更するには、**[構成（Configure）] > [SAN] > [IVR ゾーニング（IVR Zoning）] > [ゾーンセット（Zonesets）]** を選択します。ゾーンセットラジオ ボタンを選択します。**[ゾーンセットの名前を変更（Rename Zoneset）]** アイコンをクリックします。

[名前（Name）] フィールドに、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 5 ゾーンセットをアクティブ化するには、**[構成（Configure）] > [SAN] > [IVR ゾーニング（IVR Zoning）] > [ゾーンセット（Zonesets）]** を選択します。ゾーンセットラジオ ボタンを選択します。[Activate] をクリックします。

ゾーンセットの差異ウィンドウには、以前にアクティブ化された後にゾーンセットに加えられた変更を表示します。

[Activate] 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、**[構成（Configure）] > [SAN] > [IVR ゾーニング（IVR Zoning）] > [ゾーンセット（Zonesets）]** を選択します。ゾーンセットラジオ ボタンを選択します。[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。

ゾーン

ゾーンセットを選択すると、構成されているすべてのゾーンが**[ゾーン]**の下に表示されます。選択したゾーン セットに属するゾーンには、緑色のチェック ボックスが付いています。ゾーンを作成、コピー、削除、または編集できます。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。

次の表では、Cisco DCNM の **[構成] > [SAN] > [IVR ゾーニング] > [ゾーン]** 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
ゾーンの作成	ゾーンを作成します。
ゾーンのクローン処理	送信元のゾーンと同じゾーン メンバーで構成されるーンを新しい名前で作成します。
ゾーンの追加	選択したゾーンセットにゾーンを追加します。
ゾーンの削除	ゾーンセットから選択したゾーンが削除されます。
ゾーンの削除	ゾーンセットに属していない選択されたゾーンを削除します。
ゾーンの名前を変更	選択したゾーンの名前を変更します。
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、チェック ボックスがオンになっています。 **[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。
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。

フィールド	説明
スマート ゾーン	ゾーンがスマート ゾーンかどうかを指定します。 ゾーンがスマート ゾーンの場合、**true** を表示します。それ以外の場合は、**false** を表示します。 **[スマート ゾーン（Smart Zone）]** ドロップダウン リストから **[true]** または **[false]** を選択してこのフィールドを検索できます。このフィールドは、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表示されます。

Procedure

ステップ 1 ゾーンを作成するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーン]** を選択します。

ステップ 2 [ゾーンの作成（Create Zone）] をクリックします。

a) **[ゾーンの作成（Create Zone）]** ウィンドウで、ゾーンの有効な名前を入力します。

b) [作成（Create）] をクリックします。

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 3 ゾーンをクローン処理するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーン]** で、ゾーンセットを選択します。

ファブリック内のすべてのゾーンが **[ゾーン（Zones）]** の下に表示されます。**[ゾーン]** からゾーンを選択し、**[ゾーンのクローン]** をクリックします。

Note 一度にクローン処理できるデバイスは、1 つだけです。

a) **[ゾーンのクローン処理（Clone Zone）]** ウィンドウで、新しいゾーンの有効な名前を入力します。

b) [複製（Clone）] をクリックします。

クローン処理されたゾーンが **[ゾーン]** の下に表示されます。

ステップ 4 ゾーン セットの一部ではないゾーンを追加するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーンセット]** を選択し、ゾーン セットを選択します。

ファブリック内のすべてのゾーンが **[ゾーン]** の下に表示されます。**[ゾーン]** から、ゾーンセットの一部ではないゾーンを選択します。**[ゾーンの追加（Add Zone）]** アイコンをクリックします。

ゾーンセットに追加するゾーンを複数選択できます。

選択したゾーンセットにゾーンが追加されます。ゾーンセットにゾーンが追加されたことを示すために、ゾーン名の隣に緑のチェックマークが表示されます。

ステップ 5 ゾーンセットからゾーンを削除するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーンセット]** を選択します。ゾーンセットを選択します。

ファブリック内のすべてのゾーンが **[ゾーン]** の下に表示されます。**[ゾーン]** で、選択したゾーン セットに属するゾーンを選択し、**[ゾーンの削除]** をクリックします。

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 6 ゾーン セットからゾーンを削除するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーンセット]** を選択し、ゾーン セットを選択します。

ファブリック内のすべてのゾーンが **[ゾーン]** の下に表示されます。**[ゾーン]** で、選択したゾーン セットに属していないゾーンを選択し、**[ゾーンの削除]** 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、選択したゾーンを削除します。

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。

ステップ 7 ゾーンの名前を変更するには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーンセット]** を選択し、ゾーン セットを選択します。**[ゾーン]** から、名前を変更するゾーンを選択し、**[ゾーンの名前を変更]** をクリックします。

[名前] フィールドにゾーン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 8 スマート ゾーンを有効にするには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーン]** を選択します。ゾーンセットを選択します。

[ゾーン] からゾーンを選択し、**[スマート ゾーンを有効にする]** をクリックします。

[スマート ゾーン] 列の下に、**True** と表示されます。

ステップ 9 スマート ゾーンを無効にするには、**[構成] > [SAN] > [IVR ゾーニング] > [ゾーンセット]** を選択し、ゾーン セットを選択します。

[ゾーン] からゾーンを選択し、**[スマート ゾーンを無効にする]** をクリックします。

[スマート ゾーン] 列の下に、**[False]** と表示されます。

ゾーンメンバ

選択したゾーンセットとゾーンに基づいて、**[ゾーン メンバー（Zone 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。

次の表では、**[Cisco DCNM] > [Configure（構成）] > [SAN] > [IVR Zoning（IVR ゾーン分割）] > [ゾーン メンバー（Zone Members）]** エリア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
メンバーの作成とゾーンへの追加	ゾーン メンバーを作成し、ゾーンに追加します。
メンバー削除	ゾーン メンバーを削除します。一度に複数のメンバーを削除できます。
ゾーン	このメンバーが存在するゾーンを表示します。 このフィールドでゾーン名で検索できます。
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。
Name	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。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイスを指定します。 スイッチ インターフェイス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。
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。
WWN	スイッチの WWN を指定します。 スイッチの WWN を指定して検索できます。

Cisco DCNM ウェブ UI のゾーンセットからメンバーを削除または追加するには、次の手順を実行します。

Before you begin

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 ゾーン メンバーを作成して追加するには、**[Configure（構成）] > [SAN] > [IVR Zoning（IVR ゾーン分割）] > [Zone Members（ゾーン メンバー）]** を選択します。**[作成してメンバーをゾーンに追加（Create and Add Member to Zone）]** をクリックします。

a) **[メンバーの作成と追加（Create and Add Member）]** ウィンドウで、ゾーン メンバーの WWN 名[またはデバイス エイリアス（or Device Alias）] と VSANを入力します。

コロンの有無にかかわらず、WWN 名を入力できます。

Note デバイス エイリアス ゾーンにはオフライン メンバーのみを追加できます。

b) **[作成して追加（Create and Add）]** をクリックします。

作成と機能を追加では、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も利用できます。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、**[Configure（構成）] > [SAN] > [IVR Zoning（IVR ゾーン分割）] > [Zone Members（ゾーン メンバー）]** を選択します。ゾーン メンバーを選択します。**[メンバーを削除（Remove Member）]**をクリックします。

追加可能

[追加可能（Available to Add）] オプションを使用して、検出されたデバイスをゾーンに追加できます。**[メンバーの追加（Add Member）]** ダイアログには、VSAN を入力するための追加フィールドがあります。これは、通常の [ゾーニング（Zoning）] ページではなく、[IVR ゾーニング（IVR Zoning）] ページから起動した場合にのみ表示されます。

次の表では、Cisco DCNM の **[構成（Configure）] > [SAN] > [IVR ゾーニング（IVR Zoning）] > [追加可能（Available to Add）]** 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
メンバーの追加	デバイスをゾーンに追加します。
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。**[Zone By：デバイスのエイリアス（Zone By: Device Alias）]** を選択した場合、デバイスはデバイスエイリアスによってゾーンに追加されます。
タイプ	スマートゾーニングデバイスタイプを表示します。 適用できる値は**[ホスト（Host）]**と**[ストレージ（Storage）]**です。 **[ホスト（Host）]**、**[ストレージ（Storage）]** もしくは、**[タイプ（Type）]** をドロップダウ

フィールド	説明
	ンリストから選択することによってこのフィールドを検索する事ができます。
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。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイスを指定します。 スイッチ インターフェイス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。
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。
WWN	スイッチの WWN を指定します。 スイッチの WWN を指定して検索できます。

Procedure

ステップ 1 **[構成（Configure）] > [SAN] > [IVR ゾーン分割（IVR Zoning）] > [追加可能（Available to Add）]** を選択します。

ステップ 2 **[Zone by]** フィールドで、**[エンド ポート（End Ports）]** または **[デバイスのエイリアス（Device Alias）]** ラジオ ボタンを選択します。

追加できるエンド ポートまたはデバイスのリストを示すウィンドウが表示されます。

ステップ 3 ゾーンに追加するデバイスを選択します。

ステップ 4 [追加] をクリックします。

Note そのゾーンでスマート ゾーン分割が有効になっている場合は、スマート ゾーンのデバイス タイプを指定します。

複数のゾーンを選択できます。この場合、ゾーン表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。

FCIP の設定

Cisco DCNM を使用すると、ギガビット イーサネット ポート間に FCIP リンクを作成し、ファイバ チャネルの書き込みアクセラレーションと IP 圧縮を有効にすることができます。

Cisco DCNM Web UI から FCIP を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[構成（Configure）] > [SAN] > [FCIP]** を選択します。

[ようこそ（Welcome）] ページには、FCIP ウィザードを使用して FCIP を構成するためのタスクが表示されます。

ステップ 2 **[次へ（Next）]** をクリックして、スイッチ ペアを選択します。

Note 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 3 ドロップダウン リストから、**[スイッチ間（Between Switch）]** および **[スイッチ（Switch）]** で FCIP 経由で接続する 2 つの MDS スイッチを選択します。

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。

Note 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 4 **[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 5 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 6 **[次へ（Next）]** をクリックして IP アドレスを指定し、IP ルートを追加します。

ステップ 7 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。

Note **[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 8 **[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 9 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）]** : 〜 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。

  Note 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 10 **[次へ（Next）]** をクリックして、FCIP ISL を作成します。

ステップ 11 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 12 **[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 13 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 14 **[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 15 **[展開（Deploy）]** をクリックして FCIP を構成するか、**[終了（Finish）]** をクリックして構成を完了し、後で展開します。

ポート チャネル

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、リンク冗長性を提供するものです。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。

Cisco Data Center Network Manager 11.0（1）以降では、ポート チャネルを構成および編集できます。**[構成（Configure）] > [SAN] > [ポート チャネル（Port Channel）]** に移動して、ポートチャネルを作成または編集します。

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

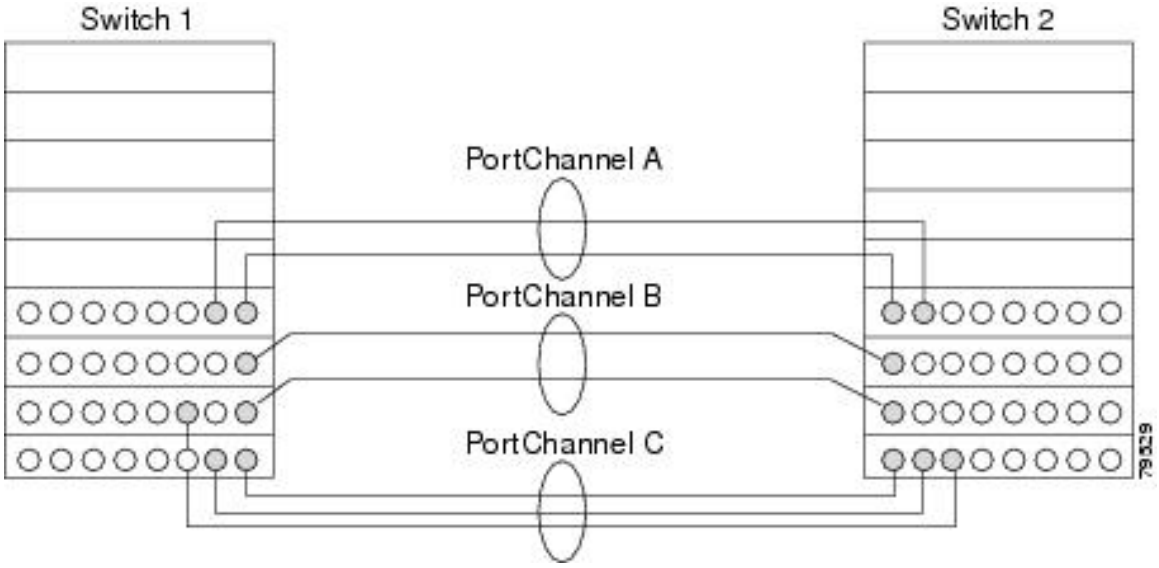
[既存のポート チャネルの編集（Edit Existing Port Channel）] をクリックしてウィザードを起動し、既存のポート チャネルを編集します。

ポート チャネルの設定に関する情報

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 *4:* 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 5 : トランキングだけ （289 ページ） および 図 6 : ポートチャネルおよびトランキング （289 ページ） を参照）。

図 *5:* トランキングだけ

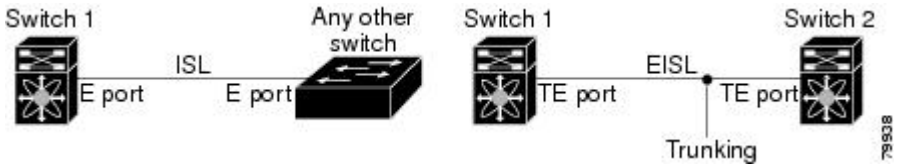
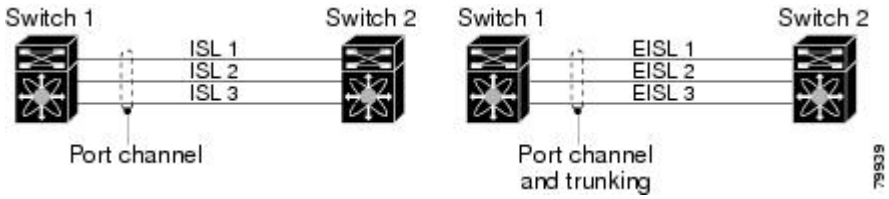


図 *6:* ポートチャネルおよびトランキング



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。

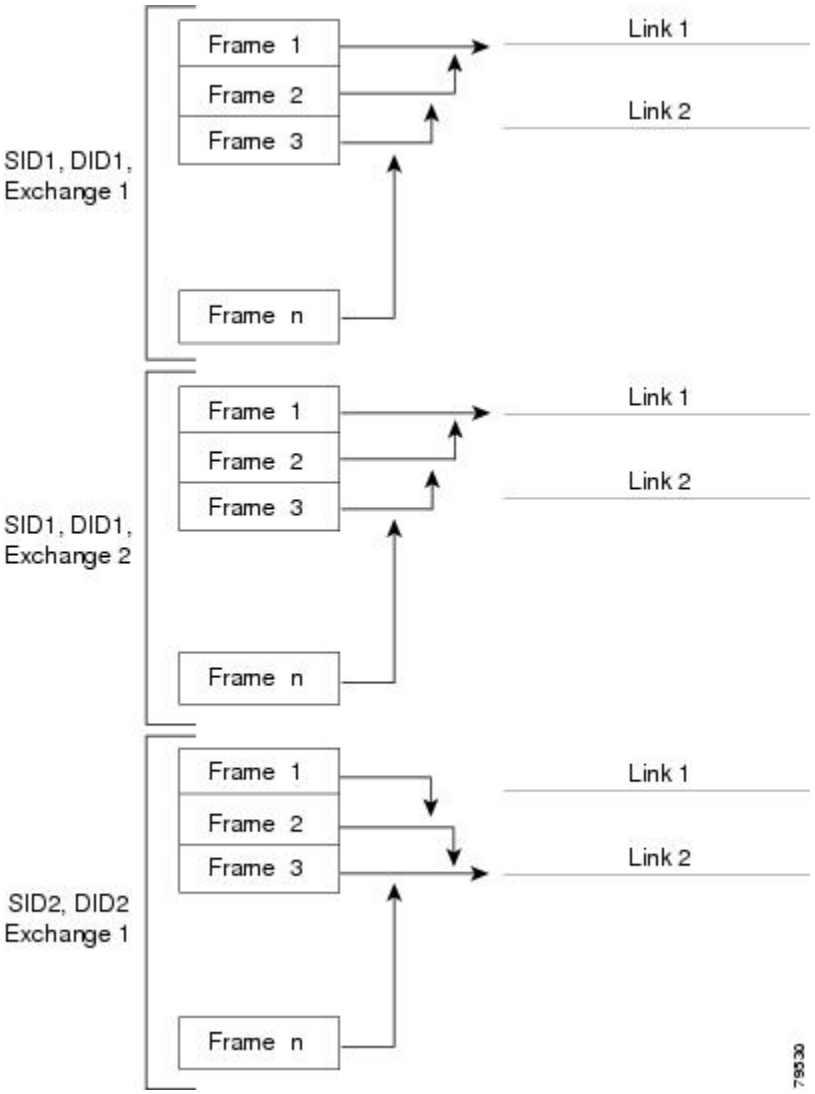
ロード バランシング

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。

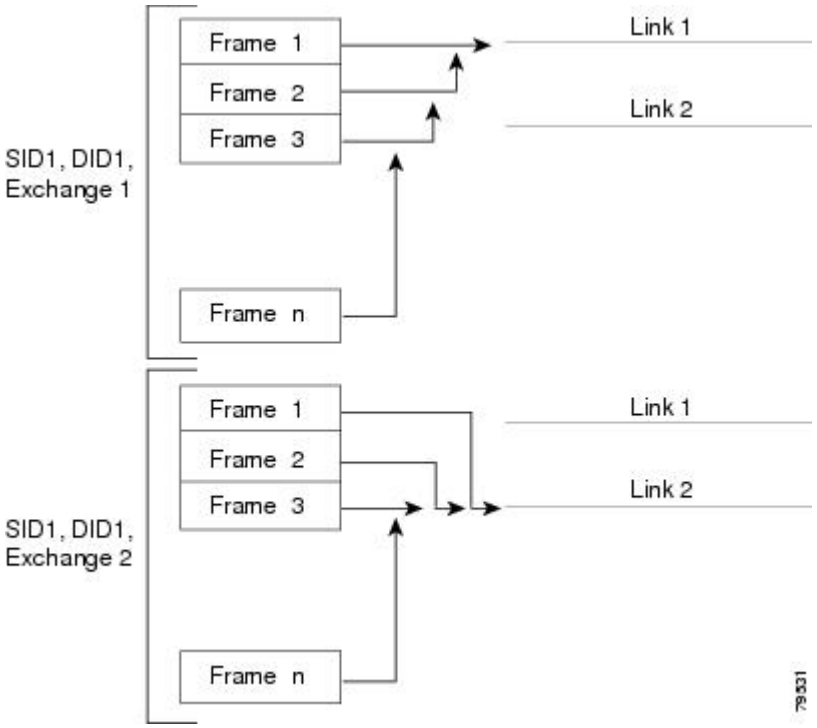
次の図に、 送信元 ID 1（SID1）と接続先 ID1（DID1）を基準とするロードバランシングの動作を示します。フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択されます。そのフローの各後続のフレームが、同一のリンク上に送信されます。SID1 および DID1 のフレームは、リンク 2 を使用しません。

図 *7: 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 *8 : 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 *29*：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。

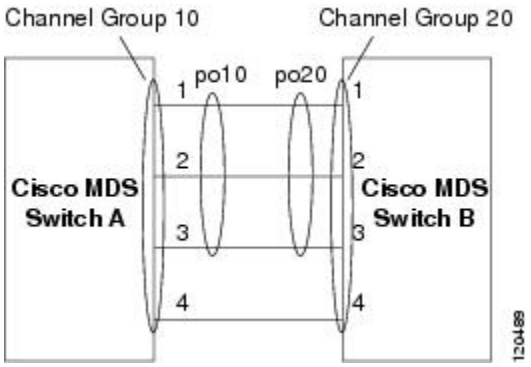
ここでは、ポートチャネルプロトコルの設定方法について説明します。ここで説明する内容は、次のとおりです。

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。

図 *9:* チャネル グループの自動作成



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。

テーブル 1-10 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。
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。

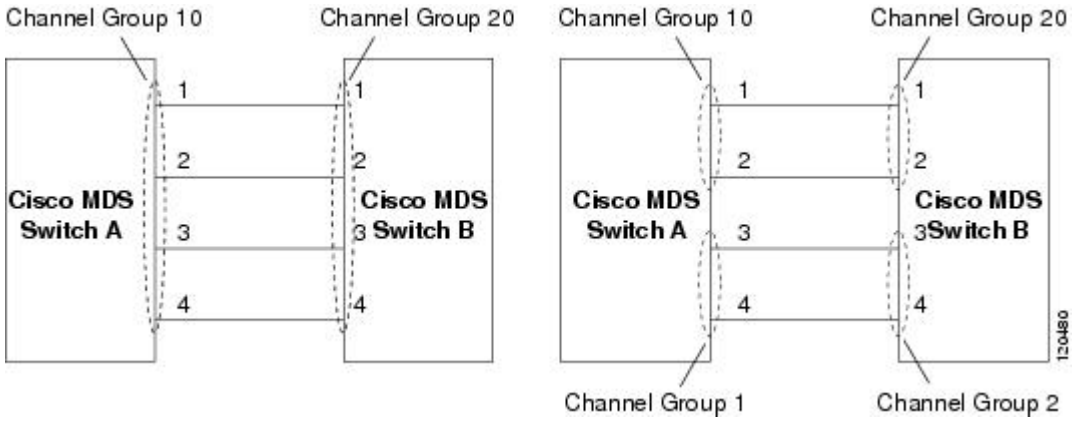
- ポートを F モードとしておく必要があります。
- 自動作成はサポートされません。
- 複数の FCIP インターフェイスを WA でグループ化する場合は、ポートチャネル インターフェイスが ACTIVE モードである必要があります。
- ON モードはサポートされません。サポートされるのは ACTIVE-ACTIVE モードだけです。デフォルトでは、NPV スイッチのモードは ACTIVE です。
- MDS スイッチの F ポートチャネル経由でログインしたデバイスは、IVR の非 NAT 設定でサポートされません。このデバイスをサポートするのは IVR NAT 設定だけです。
- ポー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

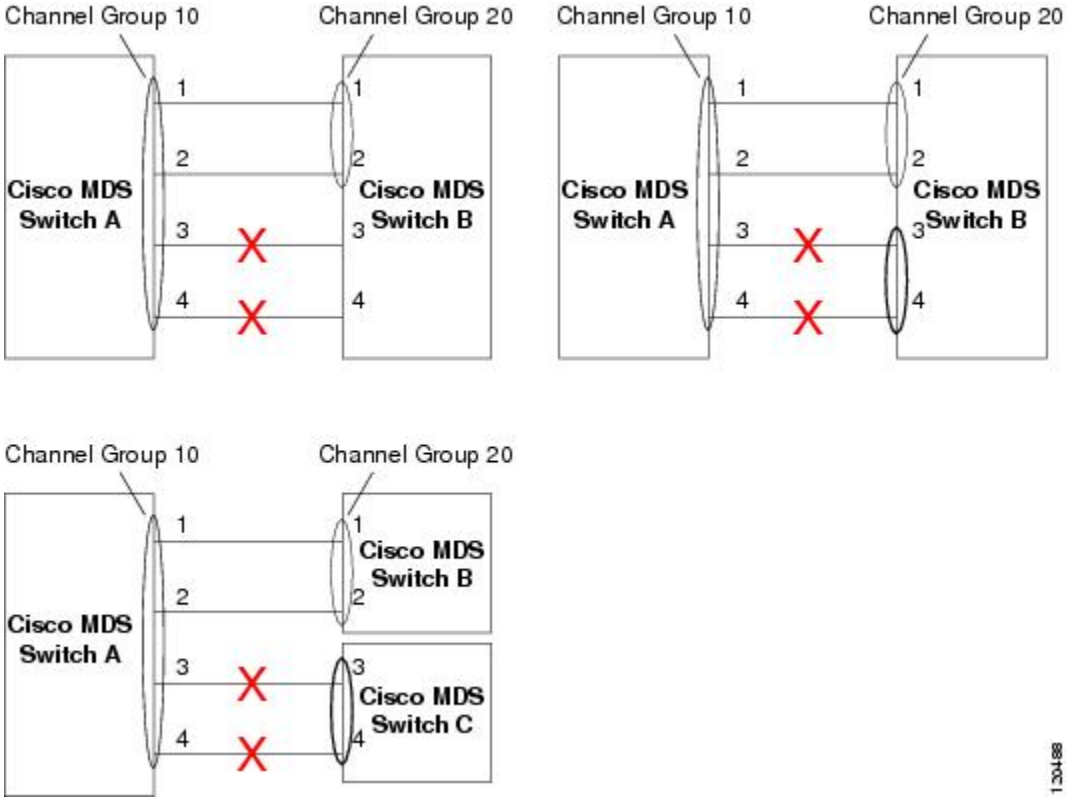
ポートチャネルは、デフォルト値で作成されます。その他の物理インターフェイスと同じように、このデフォルト設定を変更できます。次の図は、有効なポートチャネルの設定例を示しています。

図 *10*：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 *11* : 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 *30* : 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

DCNM 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 **[構成（Configure）] > [SAN] > [ポートチャネル（Port Channel）]**を選択します。

[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 ポート チャネルの作成画面で、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。**[終了（Finish）]** をクリックしてポート チャネルを構成します。

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。

ステップ 6 **[閉じる（Close）]** をクリックして、ポート チャネルの作成ウィザードを閉じます。

既知のポートチャネルの編集

DCNM 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 Cisco DCNM Web UI から、**[構成（Configure）] > [SAN] > [ポート チャネル（Port Channel）]** に移動します。

[既存のポート チャネルの編集（Edit Existing Port Channel）] をクリックし、[ポート チャネル ウィザードの編集（Edit Port Channel Wizard）] 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 **[終了（Finish）]** をクリックして、変更を適用します。

[前へ（Previous）] をクリックして、前の画面に戻り値を編集します。

[Cancel（キャンセル）] をクリックして、変更を中止します。

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。

このセクションには、**[構成] > [SAN] > [デバイス エイリアス]** の下にある状況依存のオンライン ヘルプ コンテンツが含まれています。

次の表では、**[構成] > [SAN] > [デバイス エイリアス]** 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
シード スイッチ	デバイスエイリアス シードスイッチ名を表示します。
デバイス エイリアス	シード 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。

構成

[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（Fabric）] を選択します。ファブリック上に存在するデバイス エイリアスのリストが取得され、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。

Note Cisco DCNM Web client からデバイス エイリアス構成を実行するには、ファブリックはデバイス エイリアス拡張モードとして構成する必要があります。

Procedure

ステップ 1 デバイス エイリアスを削除するには、Cisco DCNM **[Web Client] > [構成（Configure）] > [SAN] > [デバイス エイリアス（Device Alias）] > [構成（Configuration）]** タブで、削除する必要があるデバイス エイリアスをチェックします。

a) [削除（Delete）] をクリックします。

確認メッセージが表示されます。

Note 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）]** をクリックしてトピック エイリアスを削除します。

ステップ 2 デバイス エイリアスを作成するには、[Cisco DCNM **Web Client] > [構成（Configure）] > [SAN] > [デバイス エイリアス（Device Alias）] > [構成（Configuration）]** タブから、**[作成（Create）]** 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。

a) **[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。
b) **[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。
c) **[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) **[新規エイリアス（New Alias）]** をクリックして、インライン エディタ モードの新規テーブル行をクリックします。
b) **[pWWN]** フィールドで、新規エイリアスの non-provisioned port WWN 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。

Note 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 3 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（Fabric）] ドロップダウン リストから [ファブリック（Fabric）] を選択します。ファブリック上に存在するデバイス エイリアスのリストが取得され、表示されます。

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。

Cisco DCNM 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。

Procedure

ステップ 1 **[構成（Configure）] > [SAN] > [デバイス エイリアス（Device Alias）] > [CFS]** を選択します。

ステップ 2 CFS 構成をコミットするために、**[スイッチ（Switch）]** ラジオ ボタンを選択します。

[確定する（Commit）] 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 3 CFS 構成を中止するために、**[スイッチ（Switch）]** ラジオ ボタンを選択します。

[中止（Abort）] 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 4 スイッチの CFS 設定のロックを解除するには、[Switch] オプション ボタンを選択します。

[クリア ロック（Clear Lock）] 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。

ポート監視

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 DCNM 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 DCNM のユーザーは、ポリシーをプッシュする MDS スイッチの選択が許可されています。

Cisco DCNM には、ポリシーをカスタマイズするための 5 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 DCNM 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。

Note 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、**[構成（Configure）] > [SAN] > [ポート モニタリング（Port Monitoring）]** タブの Cisco DCNM に現れるフィールドについて説明します。

フィールド	説明
テンプレート	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_accessPort • Normal_allPort • Normal_trunksPort • Aggressive_accessPort • Aggressive_allPort • Aggressive_trunksPort • Most-Aggressive_accessPort • Most-Aggressive_allPort • Most-Aggressive_trunksPort • デフォルト • slowdrain

フィールド	説明
保存	ユーザー定義ポリシーの変更を保存できます。
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。 **Note** [名前を付けて保存] を選択すると、カスタマイズされたポリシーのポート タイプは保存されません。
Delete	すべてのユーザー定義のポリシーを削除できます。
スイッチにプッシュ	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。 使用可能なポートタイプは次のとおりです。 • トランク/コア • アクセスポート/エッジ • all **Note** トランクまたはすべてを選択した場合、ポート ガードは無効になります。 次のポリシーは、トランクス / コア ポリシータイプを選択します。 • Normal_trunksPort • Aggressive_trunksPort • Most-Aggressive_trunksPort 次のポリシーは、アクセスポート / エッジ ポリシータイプを選択します。 • Normal_accessPort

フィールド	説明
	• Aggressive_accessPort • Most-Aggressive_accessPort • 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。 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。 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。
カウンタの説明	カウンタ タイプを指定します。 詳細情報を表示するには、カウンタ説明の横にある「i」アイコンにポインタを移動します。
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。
下降イベント	下降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。
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。
モニタ？	デフォルト値は true です。

SAN Insights - 概要

SAN Insights の導入

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。Cisco DCNM 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。

リリース 11.2(1) からCisco DCNM 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 インサイトの全体的な拡張性を向上させます。

SAN insights ストリーミングの安定性とパフォーマンスのために『*SAN* 展開ガイドの *Cisco DCNM* インストール ガイド』にあるシステム要件セクションと、『*Cisco DCNM SAN* 管理構成ガイド』『』の柔軟な検索データベース ヒープ サイズを増加させるについてのセクションを参照します。システム RAM が十分なサイズであることを確認してください。DCNM 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。

前提条件

- 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。
- SAN Insights 機能は、小規模展開ではサポートされていません。
- フェデレーション ノードはそれぞれ 3 つの大規模な DCNM ノードで構成されている必要があります。
- SAN Insights のストリーミングの安定性とパフォーマンスのために、Elasticsearch の推奨ヒープ サイズは 16GB です。ヒープ サイズを増やすには、Elasticsearch データベース ヒープ サイズの増加 （320 ページ） を参照してください。

- 11.2(1) より古いバージョンの Cisco DCNM 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構成されている場合、スイッチは、DCNM バージョン 11.2(1) 以降でストリーミングを構成している間も、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 ストリーミング構成は、Cisco DCNM 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 DCNM Web クライアントで、**[Configure（構成）] > [SAN] > [SAN Insights]** を選択します。**[続行（Continue）]** をクリックします。適切なファブリックを選択し、**[続行（Continue）]** をクリックします。[スイッチ選択（Switch Selection）] 画面で **[分析の無効化（Disable Analytics）]** をクリックし、選択されたスイッチのすべての分析とテレメトリ構成をクリアします。

注意事項と制約事項

- SAN Insights 機能を展開するために、Cisco DCNM 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 Cisco DCNM 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 Cisco DCNM のクエリを削除します。DCNM 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。再度、Cisco DCNM から同じスイッチを設定して、新しいストリーミング間隔をプッシュします。
- HA フェデレーション モードで SAN Insights を展開するには、Elastic Search クラスタの HA パフォーマンスのために 3 ノード フェデレーション セットアップが必要です。
- 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 ダッシュボードを参照してください。

SAN Insights ダッシュボードの設定については、SAN Insights の設定 （315 ページ） を参照してください。

SAN Insights のサーバープロパティ

次の表に、プロパティ名とデフォルト値を示します。これらの値を変更するには、Web UI で **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** に移動します。

リリース 11.4(1) 以降、サーバー プロパティを更新するために、**[DCNM WebUI] > [アプリケーション（Applications）] > [カタログ（Catalog）]** ページから SAN Insights 後処理アプリケーションおよび SAN Insight パイプライン アプリケーションを停止/開始する必要はありません。アプリケーション アイコンの [一時停止（Pause）] をクリックしてから [再開（Resume）] をクリックして、サーバー プロパティに変更を適用します。

（注） サーバー プロパティに変更を適用したら、すべての DCNM サービスを再起動する必要があります。

Linux 展開の場合：次のコマンドを同じ順序で使用して、DCNM サービスを再起動します。

```
(dcnm-linux-server)# service FMServer restart
(dcnm-linux-server)# service SanInsight restart
(dcnm-linux-server)# service PIPELINE restart
```

（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 コントローラを再開してください。新しいプロパティを使用するには、SAN Insights サービスを再開してください。

表 *31 : SAN Insights* のサーバープロパティ

プロパティ名	説明	デフォルト値
san.telemetry.processing.interval	SAN Insights の処理間隔を指定します。	300,000 ミリ秒
san.telemetry.streaming.interval	SAN Insights のストリーミング間隔を指定します。	30 秒
san.telemetry.va.flow.limit	仮想マシンで DCNM を処理するために使用される一意のフロー（ITL + ITCN）の最大数を指定します。	50,000
san.telemetry.pa.flow.limit	Cisco Nexus Dashboard での処理のために取得される一意のフロー（ITL + ITCN）の最大数を指定します。	70,000
san.telemetry.use.noop.data	ECT ベースライン トレーニング計算で noop フレームを使用するかどうかを指定します。	TRUE

プロパティ名	説明	デフォルト値
san.telemetry.log.dropped	ドロップされたすべてのフローのログを明示的に指定します	FALSE
san.telemetry.train.timeframe	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.telemetry.train.reset	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.telemetry.expire.flows	フロー データが削除されるまでの保持ポリシーを指定します。	2 日間
san.telemetry.expire.flows	フロー データが削除されるまでの保持ポリシーを指定します。	7 日
san.telemetry.expire.baseline	後処理されたデータが削除されるまでの保持ポリシーを指定します。	14 日
san.telemetry.expire.rollup	時間ごとのロールアップ データが削除されるまでの保持ポリシーを指定します。	90 日
san.telemetry.expire.train	非表示のフロー トレーニング データを保持する時間を指定します	14 日
san.telemetry.deviation.low	SCSI テレメトリの偏差の低マークを指定します	10
san.telemetry.deviation.med	SCSI テレメトリの偏差メディア マークを指定します	30
san.telemetry.deviation.high	SCSI テレメトリの偏差高マークを指定します	50
san.telemetry.nvme.deviation.low	NVMe/FC テレメトリの偏差の低マークを指定します	0
san.telemetry.nvme.deviation.med	NVMe/FC テレメトリの偏差の中マークを指定します	2
san.telemetry.nvme.deviation.high	NVMe/FC テレメトリの偏差の高マークを指定します	5
san.telemetry.default.protocol	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.telemetry.gap.reset	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	正しい
san.telemetry.gap.reset.interval	レコード間の最大有効時間ギャップを指定します。	750 秒

SAN Insights の設定

Cisco DCNM Web UI から SAN insights を構成するには、次の手順を実行します。

Before you begin

Note リリース 11.3（1）以降、SAN インサイト 機能は、大規模な展開オプションのみを備えた OVA/ISO イメージを使用した Cisco DCNM 展開でサポートされます。

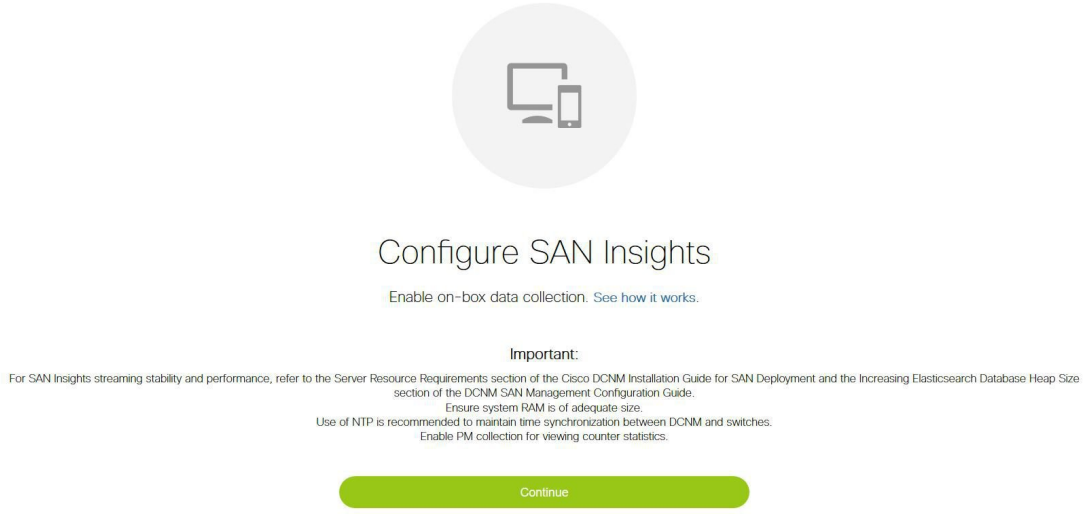
リリース 11.3(1) から、Elasticsearch ヒープ サイズはシステム RAM の合計の 25% に設定され、最大 32G のヒープ サイズになります。SAN Insights が適切に機能するには、少なくとも 16GB の Elasticsearch ヒープ サイズが必要です。OVA/ISO を使用した Cisco DCNM SAN 展開は、十分なシステム要件ですでに設定されているため、ヒープ サイズを手動で増やす必要はありません。

手順については、Elasticsearch データベース ヒープ サイズの増加, on page 320を参照してください。

Procedure

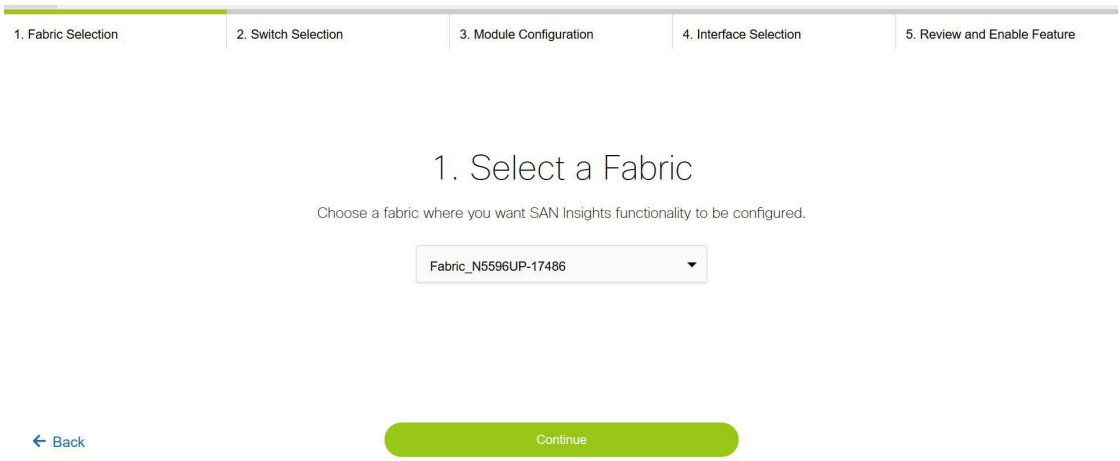
ステップ 1 **[構成（Configure）] > [SAN] > [SAN インサイト（SAN Insights）]** を選択します。

[SAN Insights の構成（Configure SAN Insights）] ウィザードが表示されます。



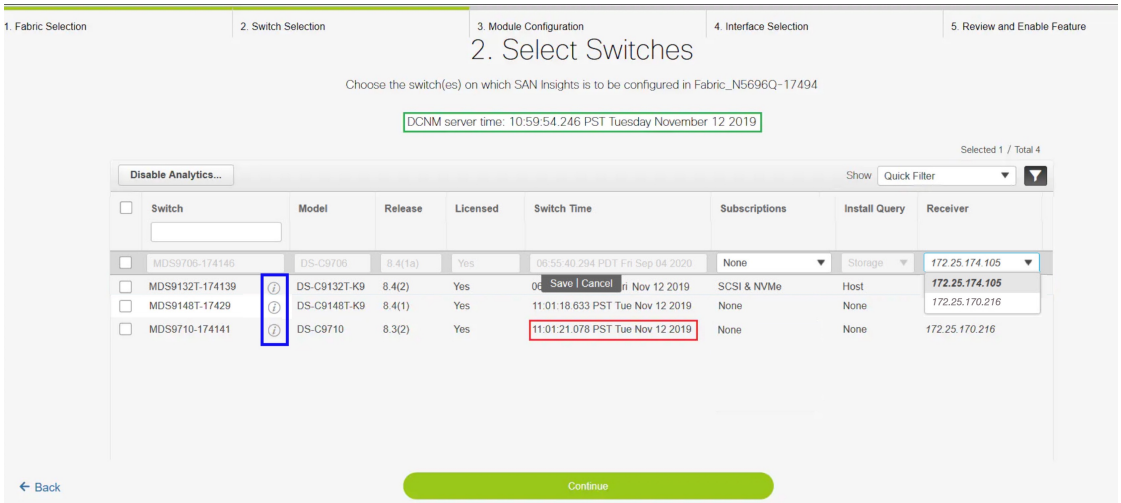
ステップ 2 **[SAN インサイトの構成（Configure SAN Insights）]** ページで、**[続行（Continue）]** をクリックします。

[ファブリック データの収集（Fabric Data Collection）] ウィンドウが表示されます。



ステップ 3 SANインサイト機能を構成するファブリックを選択します。ウィザードは一度に1つのファブリックを処理します。

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 Cisco DCNM 時間が表示され、スイッチ時間がDCNM 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。

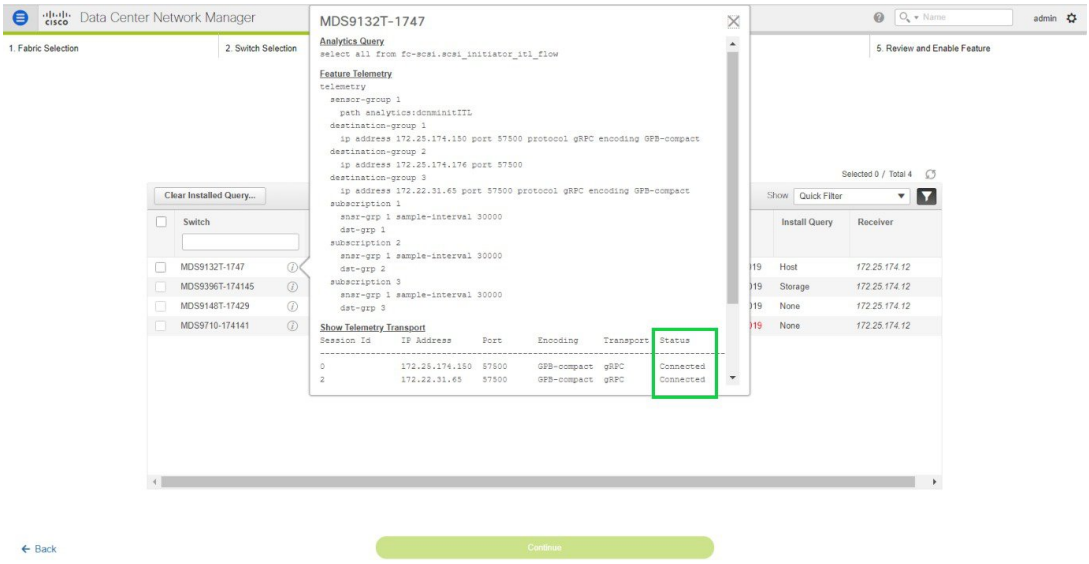
最後の列で選択された DCNM 受信者の場合、受信者はテレメトリを登録できます：SCSI のみ、NVMe のみ、SCSI と NVMe の両方、またはなし。これにより、SCSI テレメトリを受信するように 1 つの DCNM サーバを設定し、NVMe テレメトリを受信するように別の DCNM サーバを設定できます。

[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（Switch）]列の ⓘ（情報）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。



ステップ 4 **[続行（Continue）]**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 5 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、Cisco DCNM およびスイッチ時間の両方が記録され、表示されます。これは、Cisco DCNM 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。

[分析の無効化（Disable Analytics）] をクリックし、選択されたスイッチのすべての分析とテレメトリ構成をクリアします。

11.2(1) より古いバージョンの Cisco DCNM SAN インサイトを使用して、SAN インサイト ストリーミングが KVGPB エンコーディングで構成されている場合、スイッチは、DCNM バージョン 11.2（1）以降でストリーミングを構成している間も、KVGPB エンコーディングでストリーミングを継続します。Cisco DCNM リリース 11.2（1）以降、SAN インサイト のコンパクトな GPB ストリーミング構成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する必要があります。

[インストール クエリ（Install Query）] 列で、スイッチごとのポートを 1 タイプ選択し、[保存（Save）] をクリックします。**ISL**、**[ホスト（host）]**、または**[ストレージ（storage）]** のオプションから選択できます。

- **[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。

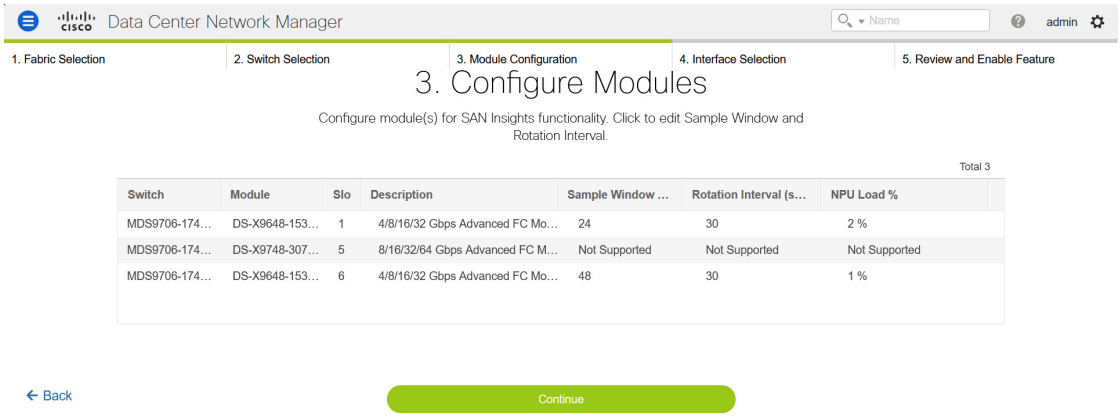
次のクエリが使用されます。

- 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 Cisco DCNM は、DCNM サーバごとに 20K（ITL＋ITN）をサポートします。ただし、重複した ITL\ITN は管理しません。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 6 **[続行（Continue）]**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）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。

リリース 11.5（4）以降、Cisco DCNM は 64G モジュールの検出をサポートしています。これらのモジュールではポートサンプリングがサポートされておらず、NPU ロードは 64G SAN 分析には適用されません。したがって、64G モジュールのサンプルウィンドウとローテーション間隔を設定することはできません。

Note 64G モジュールの場合、サンプル ウィンドウ フィールドを編集して、ポートの数を入力できます。ただし、次のエラー メッセージが表示されます。

```
Port sampling is not supported for this module.
```

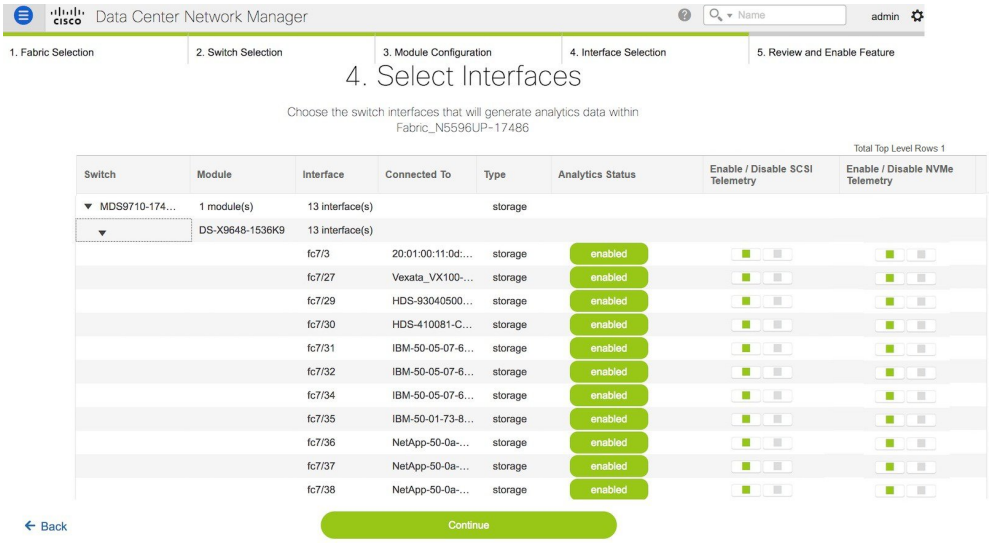
ステップ 7 **[モジュール設定（Module Configuration）]** タブで、SAN Insights 機能のモジュールを設定します。

[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 8 **[続行（Continue）]**をクリックします。

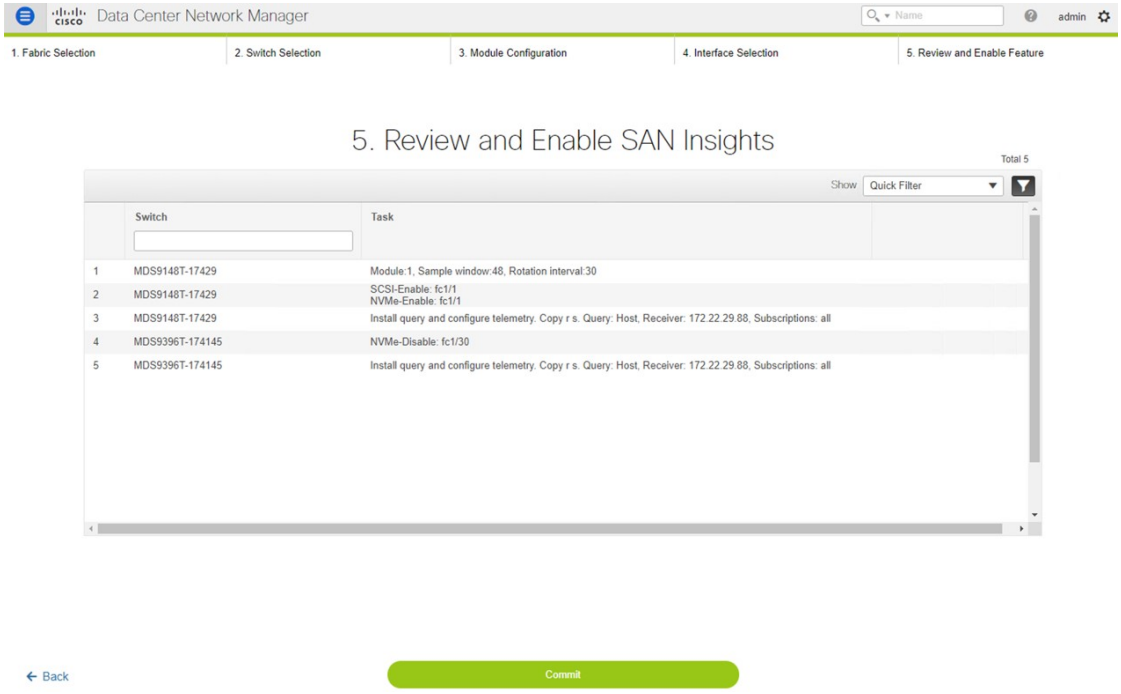


ステップ 9 **[インターフェイスの選択（Select Interfaces）]** タブで、ファブリック内で分析データを生成するインターフェイスを選択します。

インターフェイスごとに、タイプごとにテレメトリを有効または無効にすることができます。SCSI または NVMe は、SCSI のみを有効にする、NVMe のみを有効にする、SCSI と NVMe の両方を有効にする、または [なし] を各インターフェイスで有効にします。

トグルボタンをクリックして、目的のポートで分析を有効または無効にすることができます。

ステップ 10 **[続行（Continue）]** をクリックし、行った変更を確認します。



ステップ 11 [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 12 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 インサイト ページでは、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 13 **[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 **[構成（Configure）] > [SAN Insights]** ページに移動して、SAN インサイト の構成を変更します。

Elasticsearch データベース ヒープ サイズの増加

Java ヒープ サイズは、DCNM サーバー自体によって使用される Java 仮想マシンで実行されているアプリケーションに割り当てられるメモリの量です。ヒープ メモリ内のオブジェクトはスレッド間で共有でき、パフォーマンスが向上します。SAN Insights は、適切な量のヒープから恩恵を受けます。

リリース 11.3(1) 以降、Elasticsearch ヒープ サイズは、RHEL/OVA/ISO SAN デプロイメントの合計システム RAM の 25% に設定され、最大 32G のヒープ サイズになります。SAN Insights では、適切に稼働するために最小で 16GB Elasticsearch ヒープ サイズが必要です。リリース 11.3(1) では、展開時に十分なシステム RAM があれば、Elasticsearch ヒープ サイズを変更する必要はありません。

ヒープ サイズは、Linux（RHEL）SAN 展開のインストール中に設定されます。インストール時にシステム RAM が少なくなるため、Elasticsearch ヒープ サイズが 16G 未満に設定されている場合は、システム RAM を増やした後にヒープ サイズを最小の 16G に増やすことをお勧めします。

Linux CLI で Elasticsearch ヒープ サイズを指定するには、次の手順を実行します。

Procedure

ステップ 1 次のコマンドを使用して、Elasticsearch を停止します。
service elasticsearch stop

ステップ 2 vi <install-folder>/dcm/elasticsearch/config/jvm.options

ステップ 3 -Xms16g および -Xmx16g を更新し、ファイルを保存して閉じます。

ステップ 4 次のコマンドを使用して、ElasticSearch を開始します。
service elasticsearch start

Note スクリプトは、Cisco DCNM がインストールされている相対フォルダの場所にあります。

サーバーは、一定期間にわたる Elasticsearch データベース内の多数の ITL または大規模なデータセットが原因で遅くなる場合があります。このようなシナリオでは、ヒープ サイズを 32G に更新し、スレッド プールのキュー サイズを更新する必要があります。

What to do next

検索スレッド プールのキュー サイズを更新することをお勧めします。デフォルトのキュー サイズは 1000 です。

キュー サイズを 2000 に増やすには、すべてのノードで次の手順を実行します。

1. ElasticSearch サービスを停止します。
2. システムの相対インストール パスにある `elasticsearch.yml` ファイルに移動します。

   パス：<your-dcnm-install-path>
   \dcm\elasticsearch\config\elasticsearch.yml
3. `elasticsearch.yml` で、スレッド プールの検索値を 2000 に変更します。

   thread_pool.search.queue_size: 2000
4. ElasticSearch サービスを再起動します。

サービスの表示

Cisco DCNM リリース 11.3(1) 以降、SAN Insights の LINUX プラットフォームには 2 つの異なるプロセスがあります。

- パイプライン サービス
- SanInsight サービス

パイプライン サービス

LINUS プラットフォームの nexus-pipeline プロセスのステータスを確認するには、次のコマンドを実行します：

- **# service PIPELINE stop**

  パイプライン 受信者 サービスを停止します。

- **# service PIPELINE start**

  パイプライン 受信者 サービスを開始します。

- **# service PIPELINE status**

  パイプライン 受信者 サービスの実行ステータスを表示します。

SanInsight サービス

SanInsight は後処理サービスです。SanInsight プロセスのステータスを確認するには、次のコマンドを実行します。

- **# service SanInsight stop**

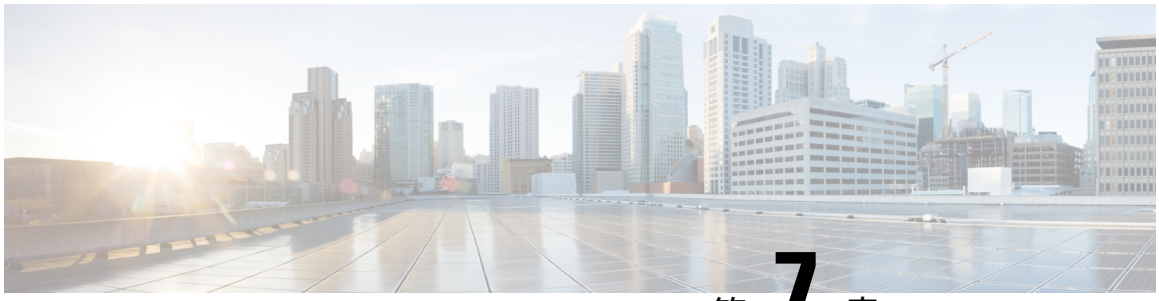
  SAN Insight ポストプロセッサ サービスを停止します

- **# service SanInsight start**

  SAN Insight ポストプロセッサ サービスを開始します

- **# service SanInsight status**

  SAN Insight ポストプロセッサ サービスの実行状態を表示します02-11-2022 04:55



第 7 章

管理（Administration）

この章は次のトピックで構成されています。

DCNM サーバ

DCNM メニューには次のサブメニューが含まれます。

サービスの開始、再開、停止

デフォルトでは DCNM とそのスイッチ間の ICMP 接続は、パフォーマンス管理中に接続を検証します。ICMP を無効にすると、パフォーマンス管理データはスイッチから取得されません。このパラメータは、**サーバー プロパティ**で構成できます。Cisco DCNM Web UI から ICMP 接続チェックを無効にするには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、`skip.checkPingAndManageable` パラメータの値を `[true]` に設定します。

Performance Manager データベース（PM DB）の古いエントリをクリーンアップし、サービスを開始、再起動、または停止するには、Cisco DCNM Web UI から、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

サーバーの詳細を表示する **[ステータス（Status）]** ウィンドウが表示されます。

ステップ 2 **[アクション]** 列で、実行するアクションをクリックします。次の操作を実行できます。

- サービスを起動または再起動します。
- サービスを停止します。
- 古い PM DB エントリをクリーンアップします。
- Elasticsearch DB スキーマを再初期化します。

ステップ 3 **[ステータス（Status）]** 列でステータスを表示します。

What to do next

[ステータス（Status）] 列で最新のステータスを確認します。

Cisco DCNM リリース 11.4(1) から、次のサービスのステータスも表示できます。

Note 次のサービスは、OVA/ISO 展開でのみ利用できます。

Windows または Linux の展開には適用されません。

- NTPD サーバー：DCNM OVA で実行されている NTPD サービス、IP アドレス、およびサービスがバインドされているポート。
- DHCP サーバー：DCNM OVA で実行されている DHCP サービス、IP アドレス、およびサービスがバインドされているポート。
- SNMP トラップ
- syslog レシーバ

これらのサービスの DCNM サーバーは次のとおりです。

サービス名	DCNM サーバー
NTPD サーバー	0.0.0.0:123
DHCP サーバー	0.0.0.0:67
SNMP トラップ	0.0.0.0:2162
[Syslogサーバ（Syslog Server）]	0.0.0.0:514

コマンド テーブルの使用

コマンド テーブルには、サーバー ステータスとサーバー管理ユーティリティ スクリプトに関する情報を提供する新しいダイアログボックスを起動するコマンドへのリンクが含まれています。これらのコマンドは、サーバー CLI で直接実行できます。

- **ifconfig**：このリンクをクリックして、Cisco DCNM サーバで使用されるインターフェイス パラメータ、IP アドレス、およびネットマスクに関する情報を表示します。
- **appmgr status all**：このリンクをクリックして、現在実行されているさまざまなサービスのステータスをチェックする DCNM サーバー管理ユーティリティ スクリプトを表示します。
- **appmgr show vmware-info**：このリンクをクリックして、仮想マシンの CPU とメモリに関する情報を表示します。
- **時計**：このリンクをクリックして、時間、ゾーン情報などのサーバー クロックの詳細に関する情報を表示します。

Note コマンド セクションは、OVA または ISO のインストールにのみ適用されます。

[カスタマイズ（Customization）]

Cisco DCNM リリース 11.3(1) 以降、Web UI ログイン ページで背景画像とメッセージを変更できます。この機能は、同時に多数のインスタンスを実行している場合に、DCNM インスタンスを区別するのに役立ちます。ログイン ページで企業ブランドの背景を使用することもできます。[デフォルトに戻す（Restore Defaults）] をクリックして、カスタマイズを元のデフォルト値にリセットします。

カスタムを削除してデフォルト値に復元するには、**[デフォルトの復元（Restore defaults）]** をクリックします。

ログイン画像

この機能では、 Cisco DCNM Web UI のログイン ページの背景画像を変更できます。DCNM のインスタンスが多数ある場合、これは、背景画像に基づいて正しい DCNM インスタンスを識別するのに役立ちます。

Cisco DCNM Web UI ログイン ページのデフォルトの背景画像を編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [カスタマイズ（DCNM Server）]** を選択します。
2. ログイン画像領域で、**[追加（+）（Add (+)）]** アイコンをクリックします。

   ローカル ディレクトリからアップロードする必要がある画像を参照します。背景画像には、JPEG、GIF、PNG、IVL、および SVG のファイル形式を使用できます。
3. 画像を選択し、**[開く（Open）]** をクリックします。

   ステータス メッセージが右下隅に表示されます。

ログイン画像アップロード成功

（注） 読み込み時間を短縮するには、拡大縮小された画像をアップロードすることをお勧めします。

アップロードされた画像が選択され、背景画像として適用されます。

4. 既存の画像をログイン画像として選択するには、画像を選択し、右下隅にメッセージが表示されるまで待ちます。
5. デフォルトのログイン画像に戻すには、**[デフォルトに戻す（Restore Defaults）]**をクリックします。

本日のメッセージ（MOTD）

この機能を使用すると、Cisco DCNM Web UI ログイン ページにメッセージを追加できます。構成された頻度でローテーションするメッセージのリストを表示できます。この機能を使用すると、ログイン ページで重要なメッセージをユーザーに伝えることができます。

Cisco DCNM Web UI ログイン ページでその日のメッセージを追加または編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバー] > [カスタマイズ（Customization）]** を選択します。
2. **[本日のメッセージ（MOTD）]**フィールドに、ログインページに表示する必要があるメッセージを入力します。
3. [保存（Save）] をクリックします。

ログ情報の表示

Performance Manager、SAN 管理サーバ、SME サーバ、Web レポート、Web サーバ、および Web サービスのログを表示できます。しかし、これらのプロセスには、ログ ファイルの情報を表示できる GUI はありません。エラーを調べる場合は、表示できるようにこれらのファイルを保存してください。

Note フェデレーション内のリモート サーバからログを表示することはできません。

Cisco DCNM Web UI からログを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [ログ（Logs）]** を選択します。

左列にログのツリーベース リストが表示されます。ツリーの下には、フェデレーション内のすべてのサーバのノードがあります。ログ ファイルは、対応するサーバ ノードの下にあります。

ステップ 2 ツリーの各ノードの下にあるログ ファイルをクリックして、右側に表示します。

ステップ 3 各サーバのツリー ノードをダブルクリックして、そのサーバからログ ファイルを含むZIP ファイルをダウンロードします。

ステップ 4 (Optional) **[テクニカル サポートの生成（Generate Techsupport）]** をクリックして、テクニカル サポートに必要なファイルを生成およびダウンロードします。

このファイルには、ログ ファイルに加えて詳細情報が含まれています。

Note OVA および ISO の展開では TAR.GZ ファイルがダウンロードされ、他のすべての展開では ZIP ファイルがダウンロードされます。 CLI で **appmgr tech_support** コマンドを使用して、techsupport ファイルを生成できます。

ステップ 5 (Optional) ログを印刷するには、右上隅の **[印刷（Print）]** アイコンをクリックします。

サーバ プロパティ

DCNM サーバで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 DCNM Web UI から DCNM 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。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

ステップ 2 **[変更を適用（Apply Changes）]** をクリックしてサーバ設定を保存します。

SFTP/SCP ログイン情報の構成

デバイス構成を収集し、構成をデバイスに復元するには、ファイル サーバーが必要です。

Cisco DCNM Web UI からファイル ストアの SFTP/SCP ログイン情報を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理] > [DCNM サーバー] > [FTP クレデンシャルのアーカイブ]** を選択します。

「**FTP ログイン情報のアーカイブ**」ウィンドウが表示されます。

Note ログイン情報は、新しい OVA および ISO インストール用に自動入力されます。

ステップ 2 **[サーバー タイプ]** フィールドで、ラジオ ボタンを使用して **SFTP** を選択します。

Note
- バックアップ操作を実行するには、SFTP サーバーが必要です。SFTP サーバーは外部サーバーにすることができます。SFTP ディレクトリは Linux/SSH の絶対パス形式である必要があり、SFTP ユーザーへの読み取り/書き込みアクセスが必要です。
- 外部サーバーを使用している場合は、**[管理] > [DCNM サーバ] > [サーバー プロパティ]** の **server.FileServerAddress** フィールドにその IP アドレスを入力します。
- **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **nat.enabled** フィールドが true の場合は、**server.FileServerAddress** フィールドに NAT デバイスの IP を入力する必要があり、SFTP サーバはローカルである必要があります。

a) [ユーザー名（User Name）] と [パスワード（Password）] に入力します。

Note リリース 11.3(1) 以降、OVA/ISO インストールの場合、**sysadmin** ユーザー ログイン情報を使用してルート ディレクトリにアクセスします。

b) **ディレクトリ** パスを入力します。

パスは Linux の絶対パス形式である必要があります。

デバイスで SFTP が使用できない場合は、ミニ SFTP、Solarwinds などのサードパーティの SFTP アプリケーションを使用できます。外部 SFTP を使用する場合は、STFP ディレクトリ パスに相対パスを指定する必要があります。たとえば、この手順の最後にあるユースケースを検討してください。

Note リリース 11.3(1) 以降、OVA/ISO インストールの場合、ディレクトリを `/home/sysadmin` として入力します。

c) **[検証スイッチ（Verification Switch）]** ドロップダウン リストから、スイッチを選択します。

d) **[適用（Apply）]** をクリックして、資格情報を保存します。

e) **[確認して適用]** をクリックして、SFTP とスイッチに接続があるかどうかを確認し、構成を保存します。

検証中にエラーが発生した場合、新しい変更は保存されません。

f) **[Clear SSH Hosts]** をクリックして、すべてのスイッチまたは選択したスイッチの SSH ホストをクリアします。

いずれかのスイッチで障害が発生すると、エラー メッセージが表示されます。**[構成] > [バックアップ] > [スイッチ構成] > [アーカイブ ジョブ] > [ジョブ実行の詳細]** に移動して、成功したスイッチと失敗したスイッチの数を表示します。

ステップ 3 **[サーバー タイプ（Server Type）]** フィールドで、ラジオ ボタンを使用して **TFTP** を選択します。

Cisco DCNM は、データ転送にローカル TFTP サーバーを使用します。DCNM サーバーで実行されている外部 TFTP サーバーがないことを確認します。

Note ユーザー切り替えの役割に copy コマンドが含まれていることを確認してください。オペレーターの役割は、許可拒否（*permission denied*）エラーを受け取ります。**[検出]** ウィンドウでログイン情報を変更できます。**[インベントリ（Inventory）] > [検出（Discovery）]** に移動します。

a) **[検証スイッチ（Verification Switch）]** ドロップダウン リストから、スイッチを選択します。
b) **[適用]** をクリックして、ログイン情報をすべての場所に保存します。
c) **[確認 & 適用]** をクリックして、TFTP とスイッチに接続があるかどうかを確認し、設定を保存します。

検証中にエラーが発生した場合、新しい変更は保存されません。

ステップ 4 **[サーバタイプ（Server Type）]** フィールドで、ラジオボタンを使用して **[SCP]** を選択します。

Note
- バックアップ操作を実行するには、SCP サーバーが必要です。SCP サーバーは外部サーバーにすることができます。SCP ディレクトリは Linux/SSH の絶対パス形式である必要があり、SCP ユーザーへの読み取り/書き込みアクセスが必要です。
- 外部サーバーを使用している場合は、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **server.FileServerAddress** フィールドにその IP アドレスを入力します。
- **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **[nat.enabled]** フィールドが true の場合は、**server.FileServerAddress** フィールドに NAT デバイスの IP を入力する必要があり、サーバーはローカルである必要があります。

a) [ユーザー名（User Name）] と [パスワード（Password）] に入力します。
b) **ディレクトリ** パスを入力します。

パスは Linux の絶対パス形式である必要があります。

デバイスで SCP を使用できない場合は、mini-SCP、Solarwinds などの外部 SCP アプリケーションを使用します。外部 SCP を使用する場合は、SCP ディレクトリ パスに相対パスを指定する必要があります。たとえば、この手順の最後にあるユース ケースを検討してください。

c) **[検証スイッチ（Verification Switches）]** ドロップダウンから、スイッチを選択します。
d) **[適用]** をクリックして、ログイン情報をすべての場所に保存します。

e) **[確認して適用（Verify & Apply）]** をクリックして、SCP とスイッチに接続があるかどうかを確認し、構成を保存します。検証中にエラーが発生した場合、新しい変更は保存されません。

f) **[Clear SSH Hosts]** をクリックして、すべてのスイッチまたは選択したスイッチの SSH ホストをクリアします。

いずれかのスイッチに障害があると、エラー メッセージが表示されます。成功したスイッチと失敗したスイッチの数を表示するには、**[構成（Configure）] > [バックアップ（Backup）] > [スイッチの構成（Switch Configuration）] > [アーカイブ ジョブ（Archive Jobs）] > [ジョブ実行の詳細（Job Execution Details）]** に移動します。

ステップ 5 **[構成（Configuration）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Templates Library）] > [ジョブ（Jobs）]** を選択して、個々のデバイスの検証ステータスを表示します。

バックアップされた構成はファイル サーバから削除され、ファイル システムに保存されます。

SFTP ディレクトリ パス

事例 1

Cisco DCNM が OVA、ISO、または Linux などの Linux プラットフォームにインストールされており、テスト フォルダが `/test/sftp/` にある場合は、SFTP ディレクトリの完全なパスを指定する必要があります。[SFTP ディレクトリ（SFTP Directory）] フィールドで、`/test/sftp` と入力します。

使用例 2：

Cisco DCNM が Windows プラットフォームにインストールされていて、テスト フォルダが `C://Users/test/sftp/` にある場合は、SFTP ディレクトリの相対パスを指定する必要があります。[SFTP ディレクトリ（SFTP Directory）] フィールドで、`/` と入力します。

次に例を示します。

- 外部 SFTP のパスが `C://Users/test/sftp/` の場合、Cisco DCNM SFTP ディレクトリ パスは `/` である必要があります。
- 外部 SFTP のパスが `C://Users/test` の場合、Cisco DCNM SFTP ディレクトリのパスは `/sftp/` である必要があります。

SCP ディレクトリ パスの例

事例 1

Cisco DCNM が OVA、ISO、または Linux などの Linux プラットフォームにインストールされていて、テスト フォルダが /test/scp/ にある場合は、SCP ディレクトリの完全なパスを指定する必要があります。**[SCP ディレクトリ（SCP Directory）]** フィールドで、`/test/scp` と入力します。

事例 2

Cisco DCNM が Windows プラットフォームにインストールされていて、テスト フォルダが C://Users/test/scp/ にある場合は、SCP ディレクトリの相対パスを指定する必要があります。**[SCP ディレクトリ（SCP Directory）]** フィールドで、/ と入力します。

次に例を示します。

- 外部 SCP のパスが C://Users/test/scp/ の場合、Cisco DCNM SCP ディレクトリ パスは / である必要があります。
- 外部 SCP のパスが C://Users/test の場合、Cisco DCNM SCP ディレクトリ パスは /scp/ である必要があります。

モジュラ デバイスのサポート

大きな変更をあまり必要としない新しいハードウェアをサポートするために、次の DCNM リリースを待たずにパッチを配布できます。**[モジュラ デバイス サポート（Modular Device Support）]**は、DCNM パッチ リリースの配布と適用に役立ちます。認証された DCNM 管理者は、パッチを本番環境のセットアップに適用できます。パッチ リリースは、次のシナリオに適用されます。

- シャーシやライン カードなどの新しいハードウェアをサポート
- 最新の NX-OS バージョンをサポート
- 重要な修正をパッチとしてサポート

Cisco DCNM Web UI からパッチの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [モジュラ デバイス サポート（Modular Device Support）]** を選択します。

ウィンドウの左側に **[DCNM サーバ（DCNM Servers）]** 列が表示され、右側に **[文殊ら デバイス サポート上布（Modular Device support information）]** ウィンドウが表示されます。

ステップ 2 **[DCNM サーバ（DCNM Servers）]**を展開して、すべての DCNM サーバを表示します。

これには、**[モジュラ デバイス サポート情報（Modular Device support information）]** テーブルのバージョン番号、対応するプラットフォーム、サポートされるシャーシ、サポートされる NX-OS バージョン、PID サポート、バックアップ ディレクトリ、および最後のパッチ展開時間とともに、インストールされたパッチのリストが含まれます。

What to do next

パッチを適用してロールバックする方法の詳細については、http://www.cisco.com/go/dcnm を参照してください。

スイッチ グループの管理

Cisco DCNM Web UI を使用して、スイッチ グループを構成できます。スイッチをグループに追加、削除、または移動したり、スイッチをグループから別のグループに移動したりできます。

この項の内容は、次のとおりです。

スイッチ グループの追加

Cisco DCNM Web UI からスイッチ グループを追加するために次の手順を実行します。

Procedure

ステップ 1 **[管理] > [DCNM サーバー] > [スイッチ グループ]** を選択します。

ステップ 2 [追加（Add）] アイコンをクリックします。

[グループを追加（Add Groups）] ウィンドウが表示され、スイッチ グループの名前を入力できます。

ステップ 3 スイッチ グループの名前を入力し、**[追加（Add）]** をクリックしてスイッチ グループの追加を完了します。

スイッチ グループ名の検証、および最大のツリーの深さは 10 です。新しいスイッチ グループを追加する前に親グループを選択しなかった場合、新しいグループは階層の最上位に追加されます。

グループまたはグループのメンバーの削除

Cisco DCNM Web UI から、グループまたはグループのメンバーを削除できます。グループを削除すると、関連するグループも削除されます。削除されたグループのファブリックまたはイーサネット スイッチは、デフォルトの SAN またはローカル エリア ネットワーク（LAN）に移動されます。

グループまたはグループのメンバーを Cisco DCNM Web UI から削除するには、次の手順を実行します。

Procedure

ステップ 1 削除するスイッチ グループまたはグループのメンバーを選択します。

ステップ 2 **[削除（Remove）]** アイコンをクリックします。

スイッチ グループまたはグループのメンバーの削除を確認するダイアログ ボックスがプロンプトします。

ステップ 3 **[はい（Yes）]** をクリックして削除するか、**[いいえ（No）]** をクリックしてアクションをキャンセルします。

スイッチ グループを別のグループに移動する

Cisco DCNM Web UI からスイッチ グループを別のグループに移動するには、次の手順を実行します。

Procedure

ステップ 1 スイッチまたはスイッチ グループを選択します。

ステップ 2 強調表示されたスイッチまたはスイッチ グループを別のグループにドラッグします。

複数のスイッチを異なるスイッチ グループ間で移動するには、**Ctrl** キーまたは **Shift** キーを使用します。

スイッチまたはスイッチ グループが表示されます。現在、ユーザーは、新しいグループの下のグループ レベルで複数のスイッチを移動することはできません。

Note グループ レベルで複数のスイッチを移動することはできません。グループとスイッチを混在させることはできません。

カスタム ポート グループの管理

カスタム ポート グループは、グループ内のインターフェイスのパフォーマンスをテストするのに役立ちます。定義されたカスタム ポートとその構成を表示できます。

このセクションは、次のトピックで構成されています。

カスタム ポート グループを追加

Cisco DCNM Web UI からカスタム ポート グループを追加するために、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

[カスタム ポート グループ（Custom Port Groups）] ウィンドウが表示されます。

ステップ 2 **[ユーザー定義グループ（User-Defined Groups）]** ブロックで、**[追加（Add）]** アイコンをクリックします。

ステップ 3 **[グループの追加ダイアログ（Add Group Dialog）]** ウィンドウで、カスタム ポート グループの名前を入力します。

ステップ 4 [追加] をクリックします。

[ユーザー定義グループ（User-Defined Groups）] 領域にカスタム ポート グループが作成されます。

スイッチおよびインターフェイスをポート グループに構成する

Cisco DCNM Web UI からのスイッチとインターフェイスを含めるようにカスタム ポート グループを構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ（User-Defined Groups）]** エリアで、スイッチとインターフェイスを追加するポート グループを選択します。

ステップ 3 **[構成（Configurations）]** エリアで、**[メンバーの追加（Add Member）]** をクリックします。

選択したカスタム ポート グループの **[ポート構成（Port Configuration）]** ウィンドウが表示されます。

ステップ 4 **[スイッチ（Switches）]** タブで、カスタム ポート グループに含めるスイッチを選択します。

使用可能な**[インターフェイス（Interfaces）]**のリストが表示されます。

ステップ 5 すべてのインターフェイスを選択して、パフォーマンスを確認します。

ステップ 6 [送信（Submit）] をクリックします。

インターフェイスのリストがカスタム ポート グループに追加されます。

ポート グループ メンバーを削除

カスタム ポート グループのポート グループ メンバーを Cisco DCNM Web UI から削除または削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 > DCNM サーバ > カスタム ポート グループ（Administration > DCNM Server > Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ]** エリアで、ポート グループを選択します。

ステップ 3 **[構成（Configuration）]** エリアで、削除する必要があるスイッチ名とインターフェイスを選択します。

ステップ 4 **[ユーザー定義グループ（User Defined Groups）]** エリアで、メンバーを削除する必要があるグループを選択します。

ステップ 5 **[メンバーを削除（Remove Member）]** 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 6 **[はい（Yes）]** をクリックして、カスタム ポート グループからメンバーを削除します。

ポート グループの削除

Cisco DCNM ウェブ UI からポート グループを除去または削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ（User Defined Groups）]** エリアで、削除する必要があるグループを選択します。

ステップ 3 **[削除（Remove）]** 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 4 **[はい（Yes）]** をクリックして、カスタム グループを削除します。

サーバー フェデレーションの表示

Note フェイルオーバーが正しく機能するためには、フェデレーション セットアップに少なくとも 3 つのノードが必要です。2 ノードのフェデレーション設定では、サーバーの 1 つがダウンしている場合、Elasticsearch はクラスタを形成できないため、Web UI は一貫性のない動作をする可能性があります。3 ノードのフェデレーション設定の場合、2 つのサーバーがダウンすると、WebUI の一貫性のない動作が見られます。

Note フェデレーションのスイッチオーバーまたはフェイルオーバーの後は、毎回ブラウザのキャッシュと Cookie をクリアするようにしてください。

Cisco DCNM でフェデレーション サーバー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 **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** を選択します。

サーバーのリストとその IP アドレス、ステータス、場所、現地時間、およびデータ ソースが表示されます。

ステップ 2 **[自動フェールオーバーを有効にする（Enable Automatic Failover）]** チェック ボックスを使用して、フェールオーバー機能をオンまたはオフにします。

ステップ 3 **[場所（Location）]** 列で、ダブルクリックして場所を編集します。

フェデレーション内のいずれかのサーバーのステータスが**非アクティブ**の場合、サーバーのステータスが**アクティブ**に変更されない限り、一部の機能が動作しないことがあります。

Note Cisco DCNM をアップグレードする前に、**[自動フェールオーバーを有効にする（Enable Automatic Failover）]** がオフになっていることを確認してください。そうしないと、フェデレーション内の 1 つのサーバーがダウンすると、デバイスは、アップグレード後に最初に起動する別の DCNM サーバーに移動されます。DCNM アップグレードの自動移動を防止するには、フェデレーション内のすべての DCNM で自動移動を無効にして、DCNM サーバーを 1 つずつアップグレードする必要があります。すべての DCNM が正常にアップグレードされ、通常通り実行された後にのみ、自動移動を再度有効にします。

Note DCNM フェデレーションでは、**[自動フェールオーバーを有効にする]** が有効になっている場合、DCNM がダウンすると、その管理下にあるデバイスが他の DCNM に移動されます。ただし、DCNM が戻った後、デバイスは元に戻りません。

Note Cisco DCNM Federation をアップグレードするときは、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** ページに再度アクセスし、アップグレードの完了後に Elasticsearch cluster sync コマンドを実行する必要があります。これにより、Elasticsearch 構成が更新され、パフォーマンスのモニタリングが再開されます。Elasticsearch cluster sync コマンドを実行するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** ページで [Elasticsearch クラスタリング（Elasticsearch clustering）] ボタンを有効にする必要があります。パフォーマンス モニタリングを再開するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー ステータス（Server Status）]** を選択し、緑色のボタンをクリックします。

ElasticSearch Cluster セクションには、エラスティック検索に関する詳細が表示されます。次のフィールドがあります。

フィールド	説明
名前	エラスティック検索クラスタの名前を指定します。

フィールド	説明
ノード	クラスタ化されたインスタンスの数を指定します。
ステータス（Status）	クラスタが有効かどうかを指定します。クラスタが有効になっていない場合、ステータスは黄色です。クラスタが有効になっている場合、ステータスは緑です。

Elasticsearch クラスタリング

Note **ElasticSearch Clustering** sync-up オプションは、フェデレーション設定のプライマリ ノードでのみ使用できます。

フェデレーション サーバーに関連付けられている各エラスティック検索ノードを Elasticsearch クラスタリングに同期するには、次の手順を実行します。

Procedure

ステップ 1 **[フェデレーション（Federation）]** ウィンドウで、**[Elasticsearch クラスタリング（ElasticSearch Clustering）]** をクリックします。**[Elastic Search クラスタリング（Elastic Search Clustering）]** ポップアップ ウィンドウが表示されます。

ステップ 2 **[適用 (Apply)]** をクリックします。
この操作により、フェデレーションサーバーに関連付けられている各エラスティック検索ノードがエラスティック検索クラスタに同期されます。この操作は、エラスティック検索をデータストアとして使用するすべての機能に悪影響を及ぼします。一部の機能は、エラスティック検索サービスの再開後に進行中のデータ同期操作の影響を受けます。

マルチ サイト マネージャ

Procedure

ステップ 1 Multi-Site-Manager（MsM）は、DCNM によってグローバルに管理されているスイッチをユーザーが検索するための単一のペインを提供します。MSM はリアルタイム検索を実行して、IP アドレス、名前、または MAC アドレスに基づいて特定の仮想マシンのトラフィックをグローバルに処理し、セグメント ID に基づいて VXLAN をサポートするスイッチを見つけることができます。スイッチのみを起動するためのハイパーリンクを提供します。このウィンドウは、

リモートサイト登録の役割も果たします。登録により、現在のDCNMサーバがリモートDCNMサーバまたはサイトにアクセスできるようになります。リモート サイトが現在の DCNM サーバにアクセスするには、リモート サイトでも登録が必要です。

ステップ 2 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。

MsMウィンドウには、リモートサイトの全体的な健全性またはステータス、およびアプリケーションの健全性が表示されます。

ステップ 3 **[スイッチ、VM IP、VM 名、MAC（Switch, VM IP, VM Name, MAC）]、[セグメント ID（Segment ID）]** で検索できます。

ステップ 4 **[+ DCNM サーバの追加（+Add DCNM Server）]** をクリックして、新しい DCNM サーバを追加できます。**[リモート DCNM サーバ情報の入力（Enter Remote DCNM Server Information）]** ウィンドウが開きます。必要な情報を入力し、**[OK]** をクリックして保存します。

ステップ 5 **[すべてのサイトの更新（Refresh All Sites）]** をクリックし、更新された情報を表示します。

ライセンスの管理

[ライセンス付与の管理 (Manage Licensing)] メニューには、次のサブメニューがあります。

ライセンスの管理

[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] を選択すると、既存のCisco DCNM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。

- ライセンスの割り当て
- スマート ライセンス
- サーバ ライセンス ファイル

Note デフォルトでは、**[ライセンスの割り当て（License Assignments）]** タブが表示されます。

次の表に、SAN および LAN のライセンス情報を示します。

フィールド	説明
License	SAN または LAN を指定します。

フィールド	説明
無料/合計サーバベースのライセンス	ライセンスの総数のうち、購入する無料ライセンスの数を指定します。新規インストールのライセンスの総数は 50 です。ただし、インライン アップグレードの場合、ライセンスの合計数は 500 のままになります。
ライセンスなし/合計（スイッチ/VDC）	スイッチまたはVDC の総数のうち、ライセンスのないスイッチまたは VDC の数を指定します。
購入する必要があります	購入するライセンス数を指定します。

このセクションは、次のトピックで構成されています。

ライセンスの割り当て

次の表に、すべてのスイッチまたは VDC のライセンス割り当ての詳細を示します。

フィールド	説明
グループ	グループがファブリックか LAN かを表示します。
スイッチ名	スイッチの名前が示されます。
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。
ライセンスの状態	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 • 評価用 • Unlicensed • N/A • 期限切れ • 無効 • スマート

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。 • DCNM サーバー • スイッチ • スマート • オナー • スイッチスマート
期限日（Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** 列の下のテキストは、7日で期限切れになるライセンスの場合は赤で表示されます。
ライセンスの割り当て	行を選択し、ツールバーのこのオプションをクリックしてライセンスを割り当てます。
割り当ての解除	ライセンスの割り当てを解除するには、行を選択し、ツールバーのこのオプションをクリックします。 **Note** ファブリック内のすべてのスイッチのライセンスの割り当てを解除すると、ファブリックもライセンスがなくなります。ただし、ファブリックのライセンスの割り当てを解除した後、フェデレーション セットアップで PM サービスを再起動して、ファブリックが **[SAN収集（SAN Collection）]** ウィンドウに表示されないようにします。ファブリックを 1 つのノードから別のノードに正常に移動するには、PM を再起動する必要があります。
すべて割り当て	ツールバーのこのオプションをクリックしてテーブルを更新し、テーブル内のすべてのアイテムにライセンスを割り当てます。
すべて割り当て解除	ツールバーのこのオプションをクリックしてテーブルを更新し、すべてのライセンスの割り当てを解除します。

Note ライセンスの割り当てまたは割り当て解除を行うには、ネットワーク管理者権限が必要です。

ファブリックが最初に検出されたときに、スイッチに有効なスイッチベースのライセンスがない場合、ライセンスはファイルライセンスプールからファブリックに自動的に割り当てられ、プール内にライセンスが残っていない状態になります。既存のファブリックがあり新しいス

イッチがファブリックに追加されたとき、ファイル ライセンス プールで使用可能なライセンスがあり、まだスイッチベースのライセンスがない場合は、新しいスイッチにライセンスが割り当てられます。

スマート ライセンスを登録した後、永久ライセンスを持たないスイッチの **[ライセンスの割り当て（Assign License）]** をクリックすると、スマート ライセンスがスイッチに割り当てられます。割り当てられるライセンスの優先順位は、次の順序です。

1. **永続**
2. **スマート**
3. **評価用**

POAP を介してスイッチにライセンスを割り当てるには、『DCNM ライセンス ガイド』を参照してください。

スマート ライセンスを無効にすると、スマート ライセンスされたスイッチのライセンスの割り当てが解除されます。

評価ライセンスは、スマートライセンスをサポートしていないスイッチに割り当てられます。ライセンス状態は **Eval** で、ライセンス タイプは **DCNM-Server** です。スマート ライセンスをサポートするスイッチのリストを表示するには、『*Cisco DCNM* ライセンス ガイド、リリース *11.x*』を参照してください。

スマート ライセンス

Cisco DCNM リリース 11.1（1）からスマート ライセンシング機能を使用して、デバイス レベルでライセンスを管理し、必要に応じて更新します。Cisco DCNM Web UI から、**管理（Smart License Administration）] > [ライセンス管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。Cisco スマート ライセンスの簡単な紹介、メニューバー、および**[スイッチ ライセンス（Switch Licenses）]**エリアが表示されます。

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。

概要で、**[ここをクリック（Click Here）]** をクリックして、スマート ソフトウェア ライセンスに関する情報を表示します。

メニューバーには次のアイコンがあります。

- **[登録状況（Registration Status）]**：クリックするとポップアップ ウィンドウに現在の登録の詳細が表示されます。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 **DEREGISTERED** に設定されます。登録後、値は **REGISTERED** に設定されます。登録ステータスをクリックして、最後のアクション、アカウントの詳細、およびその他の登録の詳細を **[登録の詳細（Registration Details）]** ポップアップ ウィンドウに表示します。
- **[ライセンスのステータス（License Status）]**: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、**AUTHORIZED** または **OUT-OF-COMPLIANCE** 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。
- **[コントロール（Control）]**：スマート ライセンスの有効化または無効化、トークンの登録、認証の更新を行うことができます。

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、**[認証済み（Authorized）]** と **[コンプライアンス違反（Out of Compliance）]** です。
説明	ライセンスのタイプと詳細を指定します。
最終更新	スイッチ ライセンスが最後に更新されたときのタイムスタンプを指定します。
プリント	スイッチ ライセンスの詳細を印刷できます。
エクスポート	ライセンスの詳細をエクスポートできます。

Cisco Smart Software Manager でアカウントから製品ライセンスを削除した後、スマート ライセンスを無効にして、再度登録します。

スマート ライセンスの有効化

Cisco DCNM Web UI からスマート ライセンスを有効にするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[コントロール（Control）]** をクリックし、ドロップダウン リストで **[イネーブル化（Enable）]** を選択して、スマート ライセンスを有効にします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックします。

DCNM インスタンスを登録する手順が表示されます。

登録ステータスが **UNCONFIGURED** から **DEREGISTERED** に変わり、ライセンス ステータスが **UNCONFIGURED** から **[使用されているライセンスはありません（No Licenses in Use）]** に変わります。

Cisco DCNM インスタンスの登録

Before you begin

Cisco Smart Software Manager のトークンを作成します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[登録（Register）]** を選択します。

[登録（Register）] ウィンドウが表示されます。

ステップ 3 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://tools.cisco.com/its/service/oddce/services/DDCEService

- **トランスポート ゲートウェイ（Transport Gateway） - ゲートウェイまたはサテライト経由のプロキシ**

  このオプションを選択する場合は、URL を入力します。

- **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 4 **[トークン（Token）]** フィールドに登録トークンを入力します。

ステップ 5 ライセンスを登録するために、**[送信（Submit）]** をクリックします。

登録ステータスが **[登録抹消（DEREGISTERED）]** から **[登録済み（REGISTERED）]** 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。

[登録ステータス：**登録済み（Registration Status: REGISTERED）]** をクリックして、登録されたトークンの詳細を表示します。

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。

What to do next

登録後に発生した通信エラーのトラブルシューティングを行います。

通信エラーのトラブルシューティング

登録中の通信エラーを解決するには、次の手順を実行します。

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 次のパスからサーバー プロパティ ファイルを開きます：/usr/local/cisco/dcm/fm/conf/server.properties

Note Windows のサーバー プロパティ ファイルは、次の場所にあります：C:/Program Files/Cisco/dcm/fm/conf/server.properties

ステップ 3 サーバー プロパティ ファイルに次のプロパティを含めます：

```
#cisco.smart.license.production=false #smartlicense.url.transport=https://
CiscoSatellite_Server_IP /Transportgateway/services/DeviceRequestHandler
```

ステップ 4 次のシンタックスで、/etc/hosts ファイルのホスト データベースにある Cisco サテライトの詳細を更新します：*Satellite_Server_IP* CiscoSatellite

ステップ 5 DCNM サービスを開始します。

認証を更新

登録済みの場合にのみ、承認を手動で更新できます。自動再承認は定期的に行われます。**[ライセンス ステータス（License Status）]** をクリックして、次回の自動再承認に関する詳細を表示します。Cisco DCNM Web UI から承認を更新するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[承認の更新（Renew Authorization）]** を選択して、ライセンス承認を更新します。

更新がある場合は、更新を取得する要求が Cisco Smart Software Manager に送信されます。更新後、**[スマート ライセンス（Smart Licenses）]** ウィンドウが更新されます。

スマート ソフトウェア ライセンスの無効化

Cisco DCNM Web UI からスマート ライセンスを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** を選択し、**[無効化（Disable）]** を選択して、スマート ライセンスを無効にします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックします。

このトークンを使用するスイッチのライセンス ステータスは、**[ライセンスの割り当て（License Assignments）]** タブで、**[ライセンスなし（Unlicensed）]** に変わります。このトークンは、Cisco Smart Software Manager の **[製品インスタンス（Product Instances）]** タブの下のリストから削除されます。

スマート ライセンスが利用できず、スマート ライセンスを無効にした場合は、**[ライセンスの割り当て（License Assignments）]** タブからライセンスを手動で解放します。

スイッチ スマート ライセンス

スマート ライセンスでスイッチが事前構成されている場合、DCNM がスイッチ スマート ライセンスを検証し割り当てます。Cisco DCNM UI を使用してスイッチにライセンスを割り当てる

には、**[管理（Administration）]>[ライセンスの管理（Manage Licensing）]>[ライセンスの割り当て（Assign License）]** または **[すべて割り当て（Assign All）]** を選択します。

（注） Cisco NX-OS リリース 9.3(6) 以降、スイッチ スマート ライセンスがサポートされます。

DCNM でスイッチ スマート ライセンスを有効にするには：

- 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、スイッチのスマート ライセンスを構成します。
- license smart register **idtoken** 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。DCNM の **[EXEC]** オプションを使用して、トークンをプッシュします。詳細については、[DCNM での EXEC モード コマンドの実行（Running EXEC Mode Commands in DCNM）]を参照してください。

ライセンスのないスイッチの場合、ライセンスは次の優先度に基づいて割り当てられます。

1. DCNM スマート ライセンス
2. DCNM サーバ ライセンス
3. DCNM 評価ライセンス

サーバ ライセンス ファイル

Cisco DCNM Web UI から、**[管理（Administration）]>[ライセンスの管理（Manage Licensing）]>[DCNM]>[サーバ ライセンス ファイル（Server License Files）]** を選択します。次のテーブルには Cisco DCNM

フィールド	説明
ファイル名	ライセンス ファイル名を指定します。
特長	ライセンス機能を指定します。
PID	製品 ID を指定します。
SAN (空き/合計)	SAN の無料ライセンス数と合計ライセンス数を表示します。
LAN (空き/合計)	LAN の無料ライセンス数と合計ライセンス数を表示します。
期限日（Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** フィールドのテキストで、7 日間で期限切れになるライセンスについては赤い色になっています。

Cisco DCNM ライセンスの追加

Cisco DCNM から Cisco DCNM ライセンスを追加するには、以下の手順を実行します。

Before you begin

次の手順を実行するには、ネットワーク管理者権限が必要です。

Procedure

ステップ 1 ライセンス ウィザードを開始するには**[管理（Administration）]>[ライセンスの管理（Manage Licensing）] > [DCNM]** を選択します。

ステップ 2 **[サーバ ライセンス ファイル（Server License Files）]** タブを選択します。

有効な Cisco DCNM-LAN [および DCNM-SAN（and DCNM-SAN）] ライセンス ファイルは表示されています。

ライセンスをロードするときは、セキュリティ エージェントが無効になっていることを確認してください。

ステップ 3 シスコから送付されたライセンス パック ファイルをローカル システムのディレクトリにダウンロードします。

ステップ 4 **[ライセンス ファイルの追加（Add License File）]** をクリックし、ローカル マシンに保存したライセンス パック ファイルを選択します。

ファイルはサーバ マシンにアップロードされ、サーバ ライセンス ディレクトリに保存されてから、サーバにロードされます。

Note .lic ファイルのコンテンツを編集しないようにしてください。編集すると、Cisco DCNM ソフトウェアでは、そのライセンス ファイルに関連付けられたすべての機能が無視されます。このファイルの内容に署名して、内容が変更されないようにする必要があります。ライセンス ファイルを間違って複数回コピー、名前変更、または挿入した場合、重複ファイルは無視されますが、元のファイルはカウントされます。

スイッチの機能：一括インストール

リリース 11.3（1）以降、Cisco DCNM 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。DCNM 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解析します。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。

Cisco DCNM 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。

1. **[管理 (Administration)] > [ライセンス付与の管理 (Manage Licensing)] > [スイッチ機能（Switch features）]** を選択します。

2. スイッチ ライセンス エリアで、**[ライセンス ファイルのアップロード（Upload License files）]** 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。

   一括でスイッチ ライセンスをインストール ウィンドウが表示されます。

3. ライセンスを選択で、**[ライセンスファイルの選択（Select License File file(s）]**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。

   [開く（Open）] をクリックします。

4. DCNM サーバからスイッチにライセンス ファイルをコピーするためのファイル転送プロトコルを選択します。

   - ライセンス ファイルをアップロードするには、**TFTP**、**SCP**、または **SFTP** プロトコルのいずれかを選択します。

（注） すべてのプラットフォームですべてのプロトコルがサポートされているわけではありません。TFTP は、Win/RHEL DCNM SAN インストールでのみサポートされます。ただし、SFTP/SCP はすべてのインストール タイプでサポートされています。

5. **VRF** 設定をサポートするライセンスの VRF チェックボックスをオンにします。

   定義済みルートの 1 つの VRF 名を入力します。

6. **[スイッチでファイルを上書きする（Overwrite file on Switch）]** チェックボックスをオンにして、アップロードされた新しいライセンス ファイルでライセンス ファイルを上書きします。

（注） overwrite コマンドは、ブート フラッシュ内の既存のファイルに新しいファイルをコピーします。以前のライセンスがすでにインストールされている場合、それはインストールを上書きしません。

7. DCNM サーバ ログイン情報で、DCNM サーバのルート ユーザー名とパスワードを入力します。

   DCNM にアクセスするための認証ログイン情報を入力します。DCNM Linux 展開の場合、これはユーザー名です。OVA\ISO 展開の場合、**sysadmin** ユーザーの資格情報を使用します。

8. [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 DCNM 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。

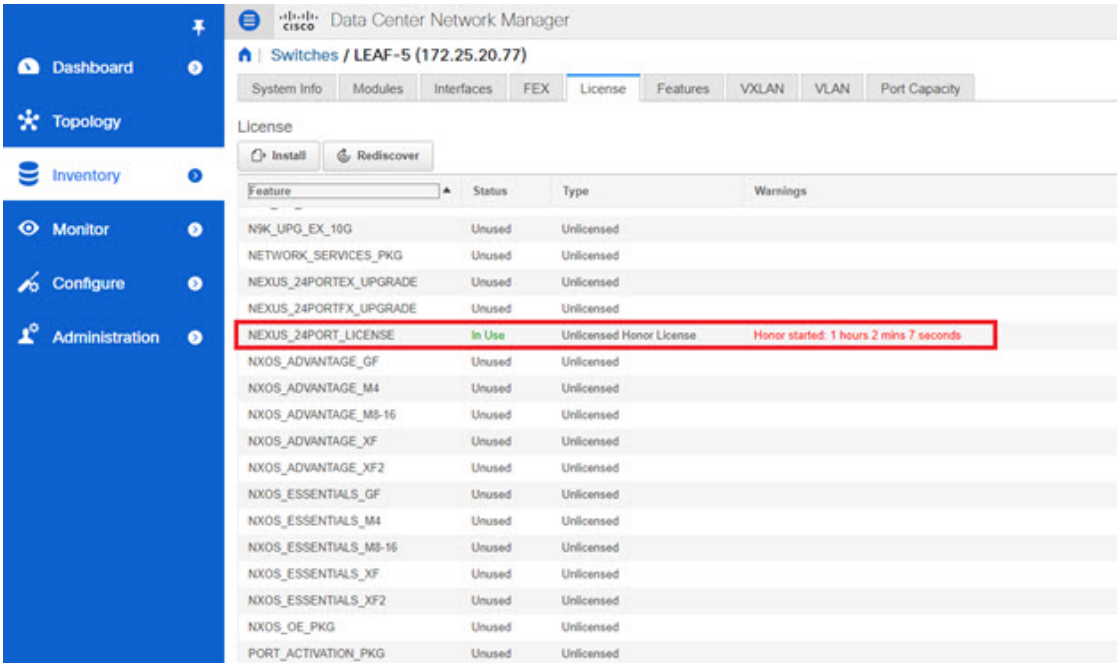
- スイッチ IP：このライセンスが割り当てられているスイッチの IP アドレス。
- ライセンス ファイル：ライセンス ファイルのファイル名
- 機能リスト：ライセンス ファイルでサポートされている機能のリスト

9. 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。
10. **[ライセンスのインストール（Install Licenses）]** をクリックします。

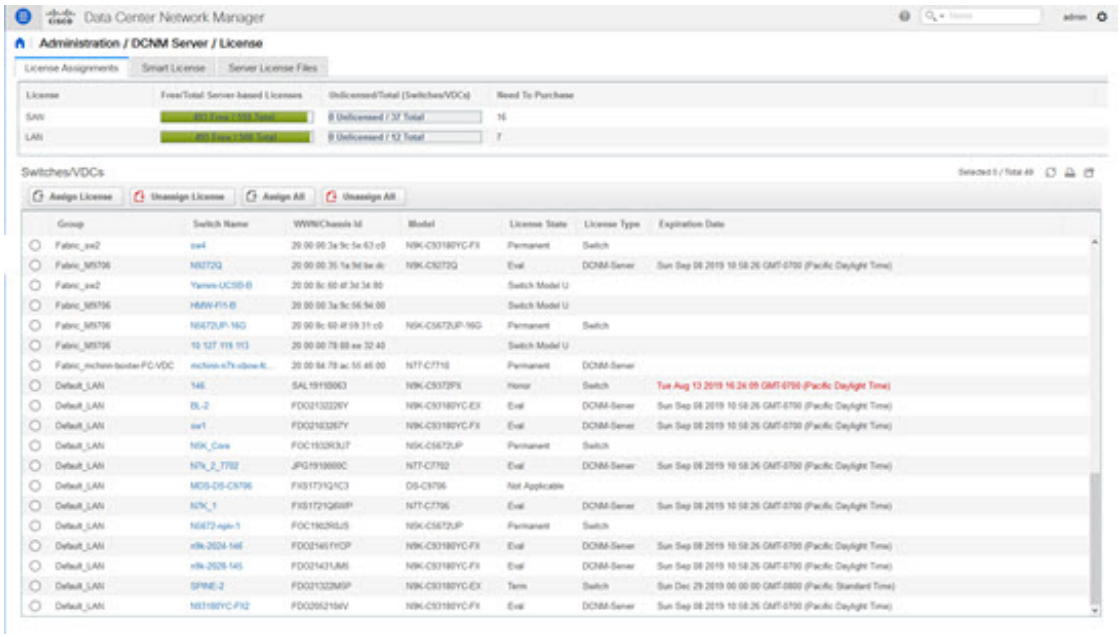
    選択したライセンスがアップロードされ、それぞれのスイッチにインストールされます。問題やエラーを含むステータスメッセージは、ファイルが完了するたびに更新されます。
11. ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ライセンスのステータス（License Status）]** テーブルにステータスが表示されます。

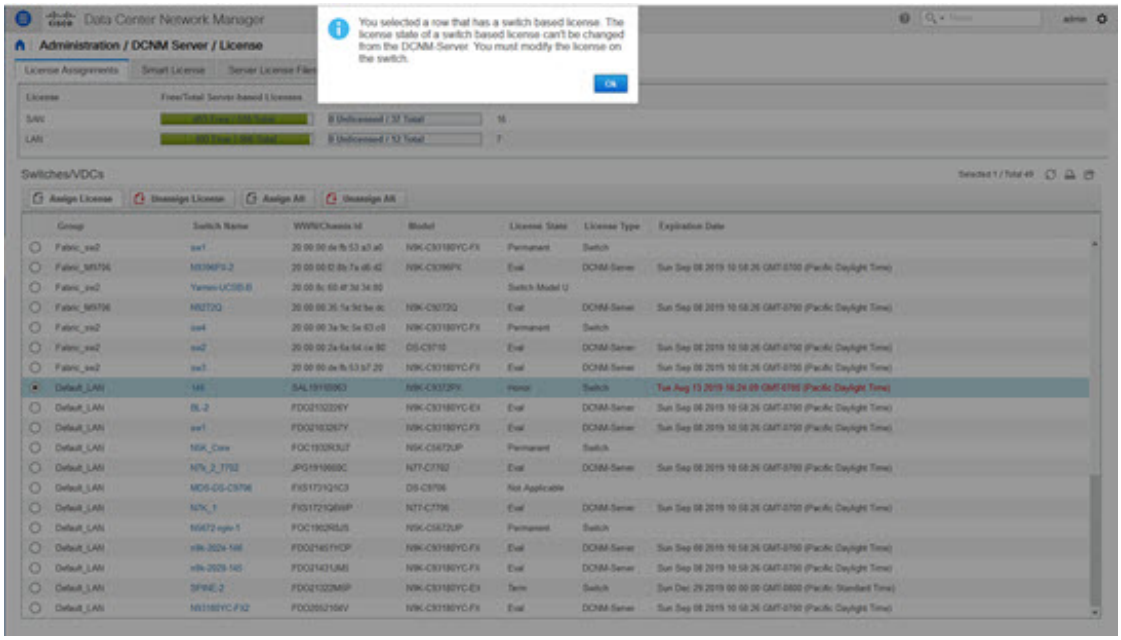
スイッチベースの名誉ライセンスのサポート

DCNM **Web UI > [インベントリ] > [スイッチ] > [ライセンス]** で、**[タイプ]** 列に「Unlicensed Honor License」と表示され、**[警告]** 列に **[Honor started: …]** と表示され、ライセンスが名誉モードに変更されてからの経過時間が表示されます。



（注） スイッチ ベースの優先ライセンスは、サーバ ベースのライセンス ファイルで上書きできません。





ユーザー管理

（注） DCNM にログインするたびに、DCNM サーバーは AAA 認証のために ISE サーバーから情報を取得します。最初のログイン後、ISE サーバは再度認証されません。

ユーザー管理メニューには、次のサブメニューがあります。

リモート AAA

Cisco DCNM Web UI からリモート AAA を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [リモート AAA プロパティ（Remote AAA Properties）]** を選択します。

AAA プロパティ構成ウィンドウが表示されます。

ステップ 2 ラジオ ボタンを使用して、次の認証モードのいずれかを選択します。

- ローカル：このモードでは、認証はローカル サーバーで認証されます。
- RADIUS：このモードでは、認証は指定された RADIUS サーバーに対して認証を行います。
- TACACS+：このモードでは、認証は指定された TACACS サーバーに対して認証を行います。
- スイッチ：このモードでは、認証は指定されたスイッチに対して認証を行います。
- LDAP：このモードでは、認証は指定された LDAP サーバーに対して認証されます。

ステップ 3 **[適用 (Apply)]** をクリックします。

ローカル

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[ローカル（Local）]** を選択します。

ステップ 2 **[適用（Apply）]** をクリックして認証モードを確認します。

RADIUS

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **Radius** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

TACACS+

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **TACACS+** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

Note IPv6 トランスポートの場合、フェールオーバーの状況中にアドレスの順序が変更されるため、AAA 認証の物理アドレスと VIP アドレスを入力します。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

スイッチ

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[スイッチ（Switch）]** を選択します。

DCNM は、IPv6 管理インターフェイスを備えた LAN スイッチもサポートします。

ステップ 2 プライマリ スイッチ名を指定し、**[適用（Apply）]** をクリックして認証モードを確認します。

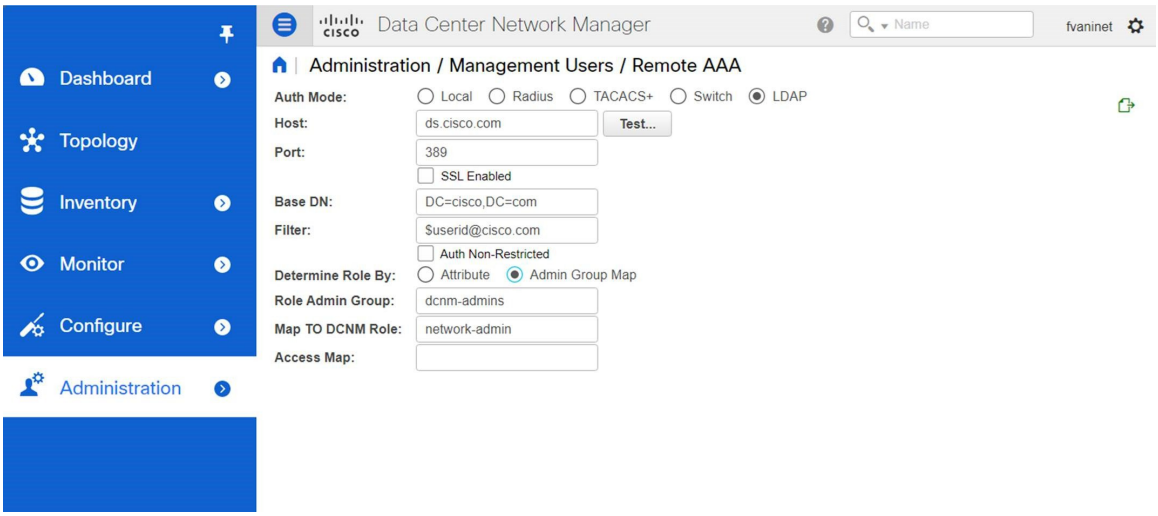
ステップ 3 (Optional) セカンダリおよびターシャリ スイッチの名前を指定します。

ステップ 4 **[適用（Apply）]** をクリックして認証モードを確認します。

LDAP

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[LDAP]** を選択します。



ステップ 2 **[ホスト（Host）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。

ドメイン ネーム システム（DNS）サービスが有効になっている場合は、LDAP サーバの DNS アドレス（ホスト名）を入力できます。

ステップ 3 [ポート（Port）] フィールドに、ポート番号を入力します。

非 SSL の場合は 389 を入力します。 SSL には 636 を入力します。デフォルトでは、ポートは非 SSL 用に構成されています。

ステップ 4 AAA サーバで SSL が有効になっている場合は、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにします。

Note LDAP over SSL を使用するには、ポートフィールドに **636** と入力し、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにする必要があります。

これで、LDAP クライアントに SSL セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの完全性と機密保持を保証します。

Note Cisco DCNM は、TLS を使用して LDAP サーバとのセキュアな接続を確立します。Cisco DCNM は、すべてのバージョンの TLS をサポートします。ただし、TLS の特定のバージョンは LDAP サーバによって決定されます。

たとえば、LDAP サーバがデフォルトで TLSv1.2 をサポートしている場合、DCNM は TLSv1.2 を使用して接続します。

ステップ 5 **[ベース DN（Base DN）]** フィールドに基本ドメイン名を入力します。

LDAP サーバはこのドメインを検索します。ベース DN は、DAP サーバで **dsquery.exe user -name**<*display_name*> コマンドを使用することで見つけることができます。

次に例を示します。

```
ldapserver# dsquery.exe users -name "John Smith"

CN=john smith,CN=Users,DC=cisco,DC=com
```

ベース DN は DC=cisco,DC=com です。

Note ベース DN 内の要素を正しい順序で入力していることを確認してください。これは、アクティブ ディレクトリ を照会するときのアプリケーションのナビゲーションを指定します。

ステップ 6 **[フィルタ処理（Filter）]** フィールドで、フィルタ処理 パラメータを指定します。

これらの値は、検索クエリをアクティブディレクトリに送信するために使用されます。LDAP 検索フィルタ文字列は最大 128 文字に制限されています。

次に例を示します。

- $userid@cisco.com

  これは、ユーザー プリンシパル名と一致します。

- CN=$userid、OU=従業員、OU=Cisco ユーザー

  これは、正確なユーザー DN と一致します。

ステップ 7 ロールを決定するオプションを選択します。**[属性（Attribute）]** または **[管理グループ マップ（Admin Group Map）]** のいずれかを選択します。

- **[管理グループ マップ（Admin Group Map）]**：このモードでは、DCNM はベース DN とフィルタ処理に基づいて、LDAP サーバにユーザーをクエリします。ユーザーがいずれかのユーザー グループに属している場合、DCNM ロールはそのユーザー グループにマッピングされます。
- **[属性（Attribute）]**：このモードでは、DCNM はユーザー属性をクエリします。属性を選択できます。**[属性（Attribute）]** を選択すると、**[ロール管理者グループ（Role Admin Group）]** フィールドが **[ロール属性（Role Attributes）]** に変わります。

ステップ 8 前の手順での選択に基づいて、**[ロール属性（Roles Attributes）]** または **[ロール管理者グループ（Role Admin Group）]** フィールドに値を入力します。

- **[管理グループ マップ（Admin Group Map）]** を選択した場合は、**[ロール管理グループ（Role Admin Group）]** フィールドに管理グループの名前を入力します。
- **[属性（Attribute）]** を選択した場合は、**[属性（Attribute）]** フィールドに適切な属性を入力します。

ステップ 9 **[DCNM ロールにマッピング（Map to DCNM Role）]** フィールドに、ユーザーにマッピングされる DCNM ロールの名前を入力します。

一般に、**network-admin** または **network-operator** が最も一般的なロールです。

次に例を示します。

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

この例では、Active Directory ユーザー グループ **dcnm-admins** を **network-admin** ロールにマップします。

複数の Active Directory ユーザー グループを複数のロールにマッピングするには、次のフォーマットを使用します：

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

[ロール管理グループ（Role Admin Group）] は空白で、**[DCNM ロールにマッピング（Map To DCNM Role）]** にはセミコロンで区切られた 2 つのエントリが含まれていることに注意してください。

ステップ 10 **[アクセス マップ（Access Map）]** フィールドに、ユーザーにマップするロール ベースのアクセスコントロール（RBAC）デバイス グループを入力します。

ステップ 11 **[テスト（Test）]** をクリックし、構成を確認します。[テスト AAA サーバ（Test AAA Server）] ウィンドウが表示されます。

ステップ 12 [テスト AAA サーバ（Test AAA Server）] ウィンドウに有効な**ユーザー名**と**パスワード**を入力します。

構成が正しい場合、次のメッセージが表示されます。

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

このメッセージは、[ロール管理グループ（Role Admin Group）] または [属性（Atribute）] モードに関係なく表示されます。これは、Cisco DCNM がクエリを Active Directory、グループ、およびロールにすることができ、を正しく構成できることを意味します。

テストが失敗すると、LDAP 認証に失敗したというメッセージが表示されます。

Warning テストが成功しない限り、構成を保存しないでください。間違った構成を保存すると、DCNM にアクセスできません。

ステップ 13 **[変更の適用（Apply Changes）]** アイコン（画面の右上隅にあります）をクリックして、構成を保存します。

ステップ 14 DCNM SAN サービスを再起動します。

- Windows の場合 – システムで、**[コンピュータの管理（Computer Management）] > [サービスとアプリケーション（Computer Management）] > [サービス（Services）]** に移動します。DCNM アプリケーションを見つけて右クリックします。**[停止（Stop）]** を選択します。1 分後、DCNM アプリケーションを右クリックし、**[開始（Start）]** を選択して DCNM SAN サービスを再起動します。

- Linux の場合 – **/etc/init.d/FMServer.restart** に移動し、リターン キーを押して DCNM SAN サービスを再起動します。

ローカル ユーザーを管理

管理者ユーザーとして、Cisco DCNM Web UI を使用して新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のグループまたは範囲を関連付けることができます。

この項の内容は、次のとおりです。

ローカルユーザーの追加

Procedure

ステップ 1 メニュー バーから**[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]**を選択します。**[ローカル ユーザー（Local Users）]** ページが表示されます。

ステップ 2 [ユーザの追加（Add User）] をクリックします。

[ユーザーを追加（Add User）] ダイアログボックスを表示します。

ステップ 3 **[ユーザー名（User name）]** フィールドにユーザー名を入力します。

Note ユーザー名は大文字と小文字が区別されますが、ユーザー名ゲストは予約済みの名前であり、大文字と小文字は区別されません。guest ユーザにできるのは、レポートの表示だけです。guest ユーザは guest パスワードを変更できず、DCNM Web クライアントの Admin オプションにもアクセスできません。

ステップ 4 **[ロール（Role）]** ドロップダウン リストからユーザーのロールを選択します。

ステップ 5 [Password] フィールドにパスワードを入力します。

Note SPACE 以外の全ての特殊文字はパスワードで許可されています。

ステップ 6 **[Confirm Password（パスワードの確認）]** フィールドで、パスワードを再入力します。

ステップ 7 **[Add（追加）]** をクリックすると、そのユーザーがデータベースに追加されます。

ステップ 8 ユーザーの追加を続行する場合は、ステップ 2 ～ 7 を繰り返します。

ローカル ユーザの削除

Cisco DCNM Web UI からローカル ユーザーを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザー（Local Users）] ページが表示されます。

ステップ 2 **[ローカル ユーザー（Local Users）]** テーブルから 1 人以上のユーザーを選択し、**[ユーザーの削除（Delete User）]** ボタンをクリックします。

ステップ 3 警告ウィンドウで **[はい（Yes）]** をクリックして、ローカル ユーザーを削除します。**[いいえ（No）]** をクリックし、削除をキャンセルします。

ユーザの編集

Cisco DCNM Web UI からユーザーを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

ステップ 2 チェックボックスを使用してユーザーを選択し、**[ユーザーの編集（Edit User）]**アイコンをクリックします。

ステップ 3 **[ユーザーの編集（Edit User）]** ウィンドウでは、デフォルトで**[ユーザー名（Username）]**と**[ロール（Role）]**が示されます。**[パスワード（Password）]** の指定と **[パスワードの確認（Confirm Password）]** をします。

ステップ 4 [適用（Apply）] をクリックし、変更を保存します。

ユーザ アクセス

ローカルユーザがアクセスできる特定のグループまたはファブリックを選択できます。これにより、ローカルユーザは、アクセスが許可されていない特定のグループまたはファブリックにアクセスできなくなります。これを行うには、次の手順を実行します。

Procedure

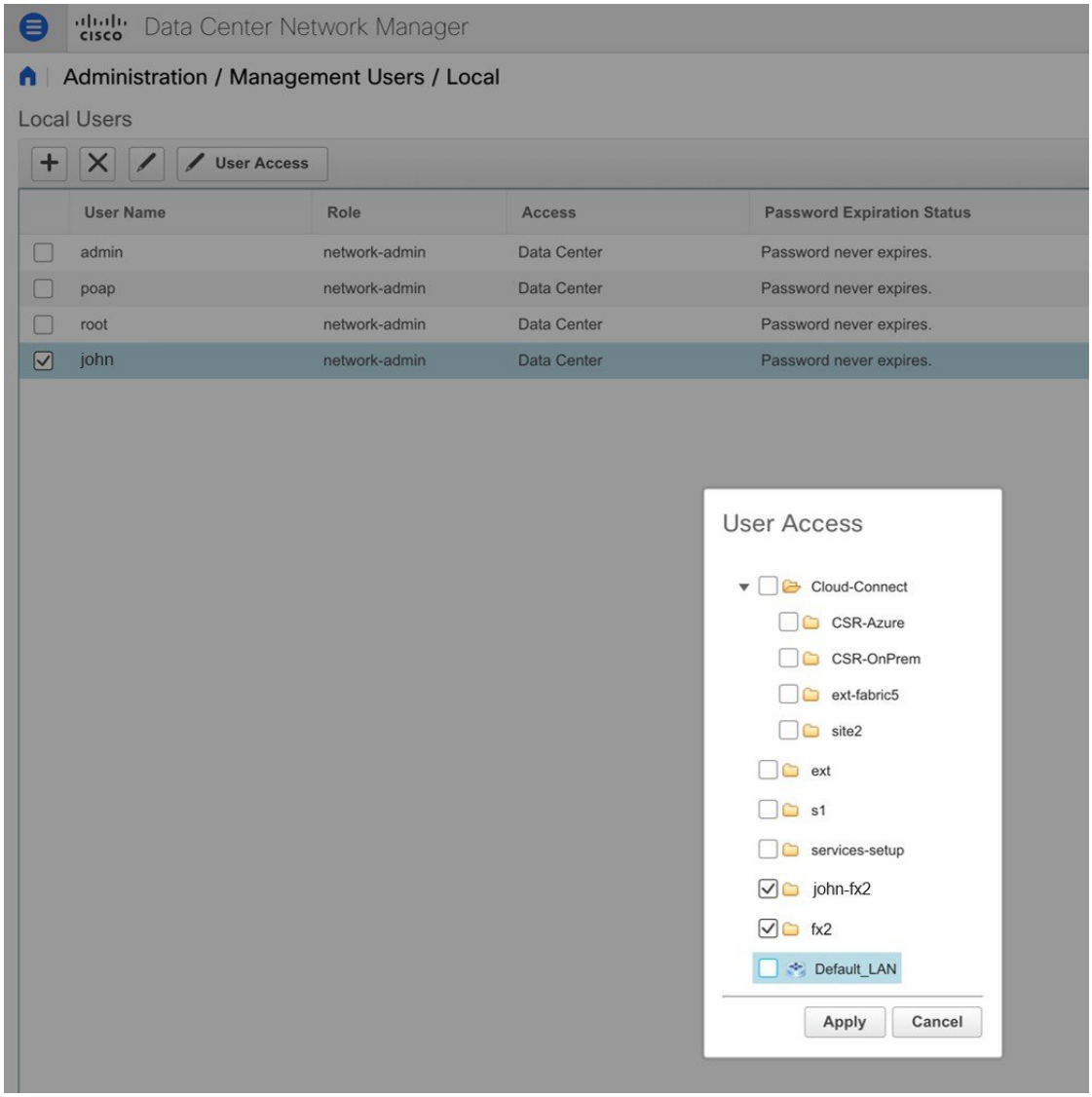
ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザ（Local Users）] ウィンドウが表示されます。

ステップ 2 **[ローカル ユーザ（Local Users）]** テーブルから一人のユーザを選択します。**[ユーザ アクセス（User Access）]** をクリックします。

[ユーザ アクセス（User Access）]選択ウィンドウが表示されます。

ステップ 3 ユーザがアクセスできる特定のグループまたはファブリックを選択し、**[適用（Apply）]** をクリックします。



クライアントを管理する

Cisco DCNM を使用して、DCNM クライアント サーバを切断できます。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [クライアント（Clients）]** を選択します。

DCNM サーバのリストが表示されます。

ステップ 2 チェックボックスを使用してDCNMサーバを選択し、**[クライアントの切断（Disconnect Client）]** をクリックして DCNM サーバを切断します。

Note 現在のクライアント セッションを切断することはできません。

パフォーマンスのセットアップ

パフォーマンスのセットアップ メニューには次のサブメニューが含まれます。

パフォーマンス セットアップ LAN 収集

Performance Manager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。Cisco DCNM を使用してパフォーマンス収集を追加または、削除することができます。スイッチの収集を作成する前に、スイッチにライセンスを付与し、**継続的な管理対象**状態に維持します。

Note Performance Manager データを収集するには、スイッチと DCNM サーバ間で ICMP ping を有効にする必要があります。**pm.skip.checkPingAndManageable** サーバ プロパティを true に設定してから、DCNM を再起動します。[Web **UI**]、**[管理（Administration）]**、**[DCNM サーバー（DCNM Server）]**、**[サーバーのプロパティ（Server Properties）]** の順に選択して、サーバ プロパティを設定します。

収集を追加する手順は、次のとおりです。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [LAN コレクション（LAN Collections）]** を選択します。

ステップ 2 ライセンスを取得したすべての LAN スイッチについて、チェック ボックスを使用して、**トランク**、**アクセス**、**エラーと破棄**、および**温度センサー**のパフォーマンス データ収集を有効にします。

ステップ 3 パフォーマンス データを収集する LAN スイッチのタイプを選択するためのチェックボックスをオンにします。

ステップ 4 [Apply] をクリックして、設定を保存します

ステップ 5 確認ダイアログボックスで、**[はい（Yes）]** をクリックして Performance Manager を再起動します。新しい設定を有効にするには、Performance Manager を再起動する必要があります。

Performance Manager SAN 収集

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。Cisco DCNM を使用してパフォーマンス コレクションを追加または、削除することができます。スイッチの収集を作成する前に、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。

収集を追加する手順は、次のとおりです。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [SAN 収集（SAN Collections）]** を選択します。

ステップ 2 ファブリックを選択して **[名前（Name）]**、**[ISL/NPV Links]**、**[ホスト（Host）]**、**[ストレージ（Storage）]**、**[FC フロー（FC Flows）]**、あるいは **[FC イーサネット（FC Ethernet）]** をこのデータ タイプのパフォーマンス収集を有効化するために選択します。

ステップ 3 [Apply] をクリックして、設定を保存します

ステップ 4 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。

パフォーマンス セットアップのしきい値

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。Cisco DCNM を使用してパフォーマンス コレクションを追加または、削除することができます。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、**managed Continuously** 状態に維持します。

Procedure

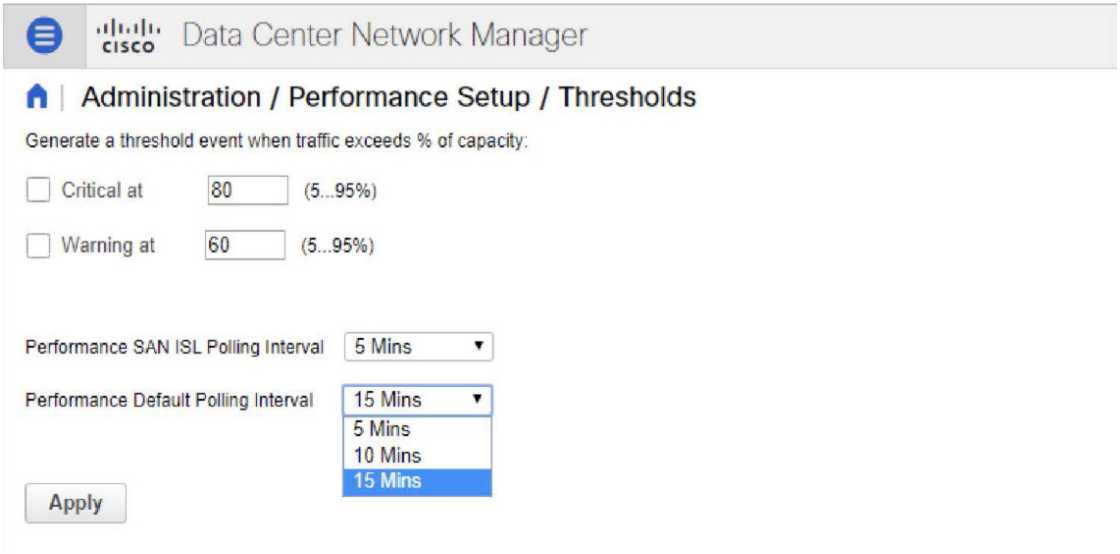
ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [しきい値（Thresholds）]** を選択します。

ステップ 2 **[トラフィックが容量の % を超えたときにしきい値イベントを生成します]** で、チェック ボックスを使用して **[重大になる時（Critical at）]** および **[警告が出る時（Warning at）]** の値を指定します。**[重大になる時（Critical at）]** の範囲は 5 ～ 95 で、デフォルトは 80 です。**[警告が出る時（Warning at）]** の範囲は 5 ～ 95 で、デフォルトは 60 です。

ステップ 3 ドロップダウン リストから **[パフォーマンス SAN ISL 投票間隔（Performance SAN ISL Polling Interval）]** の値を選択します。有効な値は、**5 分**、**4 分**、**3 分**、**2 分**、**1 分**、および **30 秒**です。デフォルトは **30 秒**です。

ステップ 4 ドロップダウン リストから **[パフォーマンス デフォルト投票間隔（Performance Default Polling Interval）]** の値を選択します。有効な値は、**5 分**、**10 分**、および **15 分**です。デフォルト値は **5 分**です。

ステップ 5 [適用（Apply）] をクリックします。



ユーザー定義の構成

Cisco DCNM Web UI からユーザー定義統計を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [ユーザー定義（User Defined）]** を選択します。

ユーザー定義の統計ウィンドウが表示されます。

ステップ 2 **[追加（Add）]** アイコンをクリックします。

[SNMP 統計をパフォーマンス収集に追加（Add SNMP Statistic to Performance Collection）] ウィンドウが表示されます。

ステップ 3 **[スイッチ（Switch）]** テーブルから、他の統計を追加するスイッチを選択します。

ステップ 4 **SNMP OID** ドロップダウン リストから、OID を選択します。

Note ドロップダウン リストから選択した SNMP OID ModuleX_Temp、IFHCInOctets.IFINDEX、IFHCOutOctest.IFINDEX の場合、「X」を正しいモジュール番号または対応する IFINDEX に置き換える必要があります。

ステップ 5 **[表示名（Display Name）]** ボックスに新しい名前を入力します。

ステップ 6 **[SNMP タイプ（SNMP Type）]** ドロップダウン リストから、タイプを選択します。

ステップ 7 **[追加（Add）]** をクリックすると、この統計が追加されます。

イベントのセットアップ

イベントのセットアップ メニューには次のサブメニューが含まれます。

イベント登録の表示

Syslog の送信、**トラップの送信**、および**トラップの遅延**を有効にするには、DCNM Web UI で次を設定する必要があります。

- **Syslog の送信**を有効にするには：**[Physical Attributes（物理的属性）] > [Events（イベント）] > [Syslog] > [Servers（サーバー）]** を選択します。**[行の作成]** をクリックし、必要な詳細を入力して、**[作成]** をクリックします。
- **送信トラップ**の有効化：**[物理属性（Physical Attributes）] > [イベント（Events）] > [SNMP トラップ（SNMP Traps）] > [送信先（Destination）]** を選択します。**[行の作成]** をクリックし、必要な詳細を入力して、**[作成]** をクリックします。
- **遅延トラップ**の有効化：**[物理属性] > [イベント] > [SNMP トラップ] > [遅延トラップ]** を選択します。**[機能の有効化]** 列で、チェック ボックスを使用してスイッチの遅延トラップを有効にし、遅延を分単位で指定します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [登録（Registration）]** を選択します。

SNMP および Syslog レシーバーと統計情報が表示されます。

ステップ 2 **[Syslog レシーバーを有効にする]** チェックボックスをオンにして **[適用]** をクリックすると、サーバー プロパティで Syslog レシーバーが無効になっている場合に有効になります。

イベント登録または syslog のプロパティを設定するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、画面の指示に従います。

ステップ 3 **[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

通知の転送

Cisco DCNM Web UI を使用して、システム メッセージの通知転送の追加および削除を実行できます。

この項の内容は、次のとおりです。

通知転送の追加

Cisco DCNM 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 サーバーでは、DCNM から SMTP サーバー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。Cisco DCNM リリース 11.4(1) 以降、DCNM により認証を必要とする任意の SMTP サーバー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。この機能を構成するには、**[管理] > [DCNM サーバー] > [サーバー プロパティ]** ウィンドウで **[SMTP] > [認証]** プロパティを設定します。**server.smtp.authenticate** フィールドに **true** を入力し、**server.smtp.username** フィールドに必要なユーザー名を入力し、**server.smtp.password** フィールドに必要なパスワードを入力します。

Cisco DCNM 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。

Note テスト転送は、ライセンスされたファブリックに対してのみ機能します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

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。

ステップ 2 イベント転送を有効にするには、**[有効にする（Enable）]** チェックボックスをオンにします。

ステップ 3 **SMTP サーバー**の詳細と**送信元**電子メール アドレスを指定します。

ステップ 4 **[適用（Apply）]** をクリックして、設定を保存します。

ステップ 5 **イベント カウント フィルタ**で、イベント カウントのフィルタをイベント フォワーダーに追加します。

イベント カウントがイベント カウント フィルタで指定された制限を超えると、転送はイベントの転送を停止します。このフィールドでは、カウント制限を指定できます。イベントを転送する前に、Cisco DCNM はその発生がカウント制限を超えていないかどうかを確認します。その場合、イベントは転送されません。

ステップ 6 **[スヌーズ]** チェックボックスを選択して、**開始**日付と時刻、**終了**日付と時刻を指定します。**[適用（Apply）]** をクリックして、設定を保存します

ステップ 7 **[イベント フォワーダー ルール（Event Forwarder Rules）]** テーブルで、**[+]** アイコンをクリックしてイベント フォワーダー ルールを追加します。

[イベント フォワーダー ルールの追加（Add Event Forwarder Rule）] ダイアログ ボックスが表示されます。

ステップ 8 **[転送メソッド（Forwarding Method）]** で、**[電子メール（E-mail）]** 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 **[ポート]** フィールドが追加されます。

ステップ 9 **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の受信者の 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 サーバー名を入力できます。

ステップ 10 **転送範囲（Forwarding Scope）** では、通知の**ファブリック/LAN** または**ポート グループ**を選択します。

ステップ 11 **[送信元]** フィールドで、**[DCNM]** または **[Syslog]** を選択します。

DCNM を選択すると、次のようになります。

a) **[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。

b) **[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。

c) **[最低重大度]** ドロップダウン リストから、受信するメッセージのシビラティ レベルを選択します。

d) **[追加（Add）]** をクリックして、通知を追加します。

[Syslog]を選択しと、次のようになります。

a) **[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。

b) syslog **タイプ**を指定します。

c) **[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。

d) **[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。

e) **[追加（Add）]** をクリックして、通知を追加します。

Note **[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 DCNM 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
```

通知の転送を削除する

通知の転送を削除できます。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

ステップ 2 削除する通知の前のチェックボックスを選択し、**[削除（Delete）]** をクリックします。

EMC CallHome の設定

Cisco DCNM Web UI から EMC がサポートする SAN スイッチの EMC Call Home を設定するには、次の手順を実行します。

Procedure

ステップ 1 **[管理] > [イベント セットアップ] > [EMC コール ホーム（EMC Call Home）]** を選択します。

ステップ 2 **[イネーブル化（Enable）]** チェックボックスを選択にして、この機能を有効にします。

ステップ 3 チェックボックスを使用して、ファブリックまたは個々のスイッチを選択します。

ステップ 4 一般的なメール情報を入力します。

ステップ 5 **[適用（Apply）]** をクリックして、E メール オプションを更新します。

ステップ 6 **[テストと適用（Apply and Test）]** をクリックして、E メール オプションを更新し、結果をテストします。

イベント抑制

Cisco DCNM では、ユーザー指定のサプレッサ 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 DCNM 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DCNM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。

Note Cisco DCNM Web UI から EMC Call Home イベントを抑制することはできません。

このセクションの内容は次のとおりです。

イベント抑制ルールの追加

Cisco DCNM 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。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

[抑制（Suppression）] ウィンドウが表示されます。

ステップ 2 **[イベント抑制（Event Suppressors）]** テーブルの上にある **[追加（Add）]** アイコンをクリックします。

[イベント抑制ルールの追加（Add Event Suppressor Rule）] ウィンドウが表示されます。

ステップ 3 **[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ウィンドウで、ルールに **Name** を指定します。

ステップ 4 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（LAN, 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（Port Group）]** 範囲のグループのみ選択できます。範囲として **[任意（Any）]** を選択する場合、抑制ルールはグローバルに適用されます。

ステップ 5 **Facility** 名を入力するか、**SAN/LAN Switch Event Facility** 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。

ステップ 6 ドロップダウン リストから、[イベント**Type**（Event）] 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。

ステップ 7 **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。

ステップ 8 **[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。

Note 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 DCNM 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、DCNM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、**[抑制（Suppressor）]** テーブルに移動し、**[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ダイアログ ウィンドウを呼び出します。

Note **[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択して、既知のイベントの抑制ルールを作成します。アカウンティングイベントの抑制ルールを作成する際にショートカットはありません。

イベント抑制ルールを削除

Cisco DCNM Web UI からイベント抑制ルールを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 > イベントをセットアップ > 抑制（Administration > Event Setup > Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[Delete（削除）]**アイコンをクリックします。

ステップ 3 確認のために [はい（Yes）] をクリックします。

イベント抑制ルールの変更

イベント抑制ルールを変更するには、次のタスクを実行します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[編集（Edit）]** をクリックします。

[施設（Facility）]、**[タイプ（Type）]**、**[説明一致（Description Matching）]**文字列、および**[有効な時間範囲（Valid time range）]**を編集できます。

ステップ 3 **[適用（Apply）]** をクリックして、変更内容を保存します。

クレデンシャル管理

ユーザー ログイン情報管理メニューには、次のサブメニューがあります：

SAN 資格情報

Cisco DCNM ホームページで、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 資格情報（SAN Credentials）]** を選択すると、ファブリック シード スイッチへの SNMP アクセスの詳細が表示されます。ユーザー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 資格情報が表示されます。

Cisco DCNM のスイッチ資格情報ウィンドウには、次のフィールドがあります。

フィールド	説明
Fabric Name（ファブリック名）	スイッチが属するファブリック名を表示します。

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（User Name）]	Cisco DCNM のユーザーのユーザー名を指定します。
[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 DCNM ユーザーが SNMP を使用してファブリックを設定する前に、ユーザーはファブリックのシード スイッチに SNMP 資格情報を提供し、検証する必要があります。ユーザーがファブリック シードスイッチの有効な資格情報を提供しない場合、[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。

スイッチの行をクリックして、正しい資格情報を入力します。**[保存（Save）]**をクリックして変更内容を保存します。

ユーザーが構成を変更しても、有効なスイッチ資格情報を提供しない場合、ユーザーアクションは拒否されます。スイッチの資格情報を検証して、変更をコミットします。

この画面で次の操作を実行できます。

- 資格情報を再検証するには：
  1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 情報管理（SAN Credentials）]** を選択し、**[ファブリック名（Fabric Name）]** オプション ボタンをクリックして、資格情報を検証する必要があるシード スイッチを選択します。
  2. [再検証（Revalidate）] をクリックします。

     操作が成功したか失敗したかを示す確認メッセージが表示されます。

- スイッチ資格情報をクリアします。
  1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 情報管理（SAN Credentials）]** を選択し、**[ファブリック名（Fabric Name）]** オプション ボタンをクリックして、シード スイッチを選択し削除します。

2. [Clear] をクリックします。

   確認メッセージが表示されます。

3. **[はい（Yes）]** をクリックして、DCNM サーバからスイッチ資格情報を削除します。

LAN 資格情報

デバイス構成の変更中、Cisco DCNM はユーザーから提供されたデバイスの資格情報を使用します。ただし、LAN スイッチ資格情報がプロビジョニングされない場合、Cisco DCNM では **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** ページを開き、LAN 資格情報を構成するようにプロンプトが表示されます。

Cisco DCNM は、次の 2 つのログイン情報のセットを使用して ローカル エリア ネットワーク（LAN）デバイスに接続します。

- **[ディスカバリ資格情報（Discovery Credentials）]**：Cisco DCNM は、デバイスの検出および定期的なポーリング中にこれらのログイン情報を使用します。
- **[構成変更ログイン情報（Configuration Change Credentials）]**：ユーザーがデバイス構成を変更する機能を使用しようとすると、Cisco DCNM はこれらのログイン情報を使用します。

LAN ログイン情報管理では、構成変更ログイン情報を指定できます。LAN スイッチの構成を変更する前に、スイッチの構成変更 SSH ログイン情報を入力する必要があります。ログイン情報を提供しない場合、構成変更アクションは拒否されます。

これらの機能は、LAN ログイン情報機能からデバイス書き込みログイン情報を取得します。

- アップグレード（ISSU）
- メンテナンス モード（GIR）
- パッチ（SMU）
- テンプレートの展開
- POAP-Write erase reload、Rollback
- インターフェイスの作成/削除/設定
- VLAN の作成/削除/設定
- VPC ウィザード

デバイスが最初に検出されたかどうかに関係なく、構成変更のログイン情報を指定する必要があります。これは1回限りの操作です。ログイン情報が設定されると、構成変更操作に使用されます。

Default Credentials

デフォルトのログイン情報は、ユーザーがアクセスできるすべてのデバイスに接続するために使用されます。スイッチテーブルのデバイスそれぞれにログイン情報を指定して、デフォルトのログイン情報を上書きできます。

Note **[パスワード（Password）]**、**[パスワードの確認（Confirm Password）]** フィールドに適切なログイン情報を入力して **[保存（Save）]** をクリックした後、**[パスワードの確認（Confirm Password）]** フィールドが空白です。空白の **[パスワードの確認（Confirm Password）]** フィールドは、パスワードが正常に保存されたことを意味します。

Cisco DCNM はまず、[スイッチ（Switch）] テーブルの個別のスイッチログイン情報を使用しようとします。[スイッチ（Switch）] テーブルの資格情報（ユーザー名/パスワード）列が空白の場合、デフォルトのログイン情報が使用されます。

スイッチテーブル

スイッチテーブルは、ユーザーがアクセスしたすべてのローカルエリアネットワーク（LAN）スイッチをリストにします。デフォルトのログイン情報を上書きするスイッチログイン情報を個別に指定できます。ほとんどの場合、デフォルトのログイン情報のみを入力する必要があります。

この画面で次の操作を実行できます。

- ログイン情報の編集, on page 372
- ログイン情報の検証, on page 372
- スイッチログイン情報のクリア, on page 372
- リモート アクセスによる認証情報管理, on page 372

DCNM ユーザーの ローカル エリア ネットワーク（LAN）ログイン情報テーブルには、次のフィールドがあります。

フィールド	説明
スイッチ	ローカルエリアネットワーク（LAN）スイッチ名を表示します。
IP アドレス	スイッチの IP アドレスを指定します。
[ユーザ名（User Name）]	スイッチ DCNM ユーザーのユーザー名を指定します。
パスワード	SSH パスワードの暗号化形式を表示します。
グループ	スイッチが属するグループを表示します。

ログイン情報の編集

次のタスクを実行して、ログイン情報を編集します。

1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）資格情報（LAN Credentials）]** を選択し、ログイン情報を編集する必要がある **[スイッチ（Switch）]** チェック ボックスをオンにします。
2. [Edit] アイコンをクリックします。
3. スイッチに **[ユーザー名（User Name）]** および **[パスワード（Password）]** を指定します。

ログイン情報の検証

ログイン情報を検証するには、次のタスクを実行します。

1. **[管理（Administration）] > [ログイン情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）ログイン情報（LAN Credentials）]** から、ログイン情報を検証する必要がある **[スイッチ（Switch）]** チェック ボックスを選択します。
2. [**Validate**] をクリックします。

   操作が成功したか失敗したかを示す確認メッセージが表示されます。

スイッチログイン情報のクリア

次のタスクを実行して、スイッチ ログイン情報をクリアします。

1. **[管理（Administration）] > [ログイン情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN） ログイン情報（LAN Credentials）]**から、ログイン情報をクリアする必要がある **[スイッチ（Switch）]** チェック ボックスをオンにします。
2. [Clear] をクリックします。
3. **[はい（Yes）]** をクリックして、DCNM サーバからスイッチ ログイン情報をクリアします。

リモート アクセスによる認証情報管理

DCNM では、次のようなさまざまなモードでユーザーを認証できます。

- ローカル ユーザ ー- このモードでは、Cisco DCNM Web UI を使用して、新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のファブリックまたはグループへのアクセス権を提供できます。
- リモート ユーザー - このモードでは、DCNM にログインできます。DCNM サーバーは、AAA 認証のために、リモート認証サーバー（Cisco Identity Services Engine（ISE）など）から情報を取得します。シスコは、リモート認証用に TACACS+、RADIUS、および LDAP オプションをサポートしています。詳細については、「リモート AAA」を参照してください。

リモート認証用に DCNM を構成すると、AAA サーバーは認証と認可の両方を処理します。DCNM は、認証を確認するために入力されたユーザ ログインとパスワードを AAA サーバーに転送します。認証後、AAA サーバーは **cisco-avpair** 属性を介してユーザーに割り当てられた適切な権限/ロールを返します。この属性には、特定のユーザーがアクセスできるファブリックのリストを含めることができます。DCNM LAN 展開でサポートされるロールは次のとおりです。

- network-admin
- network-operator

デバイス検出資格情報と LAN 資格情報はどちらもデバイスへの書き込みアクセス権を提供しますが、書き込み操作は LAN 資格情報でのみ実行されるため、両者は異なります。デバイス検出資格情報は各デバイスに関連付けられ、デバイスを DCNM にインポートするときに 1 回だけ入力されます。DCNM は、デバイスへの SSH アクセスと SNMPv3 アクセスを組み合わせて使用する定期的な再検出に、これらの資格情報を使用します。ただし、LAN 資格情報は、ユーザーごとにすべてのユーザーに対して構成されます。適切なロールを持つユーザーが DCNM にアクセスする場合、そのユーザーは LAN 資格情報を入力してデバイスへの書き込みアクセス権を取得できます。書き込み操作では、LAN 資格情報を使用してデバイスにアクセスします。これにより、すべてのユーザーが DCNM で行った変更と、その結果としてデバイスに加えられた変更の適切な監査証跡が得られます。

TACACS+ や RADIUS などのリモート認証方式を使用して DCNM を設定する場合、ユーザーは次のように LAN 資格情報を構成できます。

- 通常の AAA リモート認証
- AAA リモート認証パススルー メカニズム
- DCNM サービス アカウントを使用した AAA リモート認証

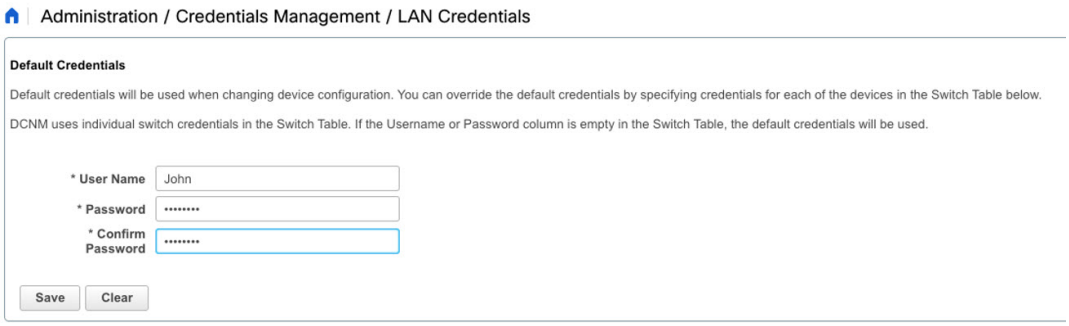
通常の AAA リモート認証

認証後、適切なロールを持つユーザーが初めて DCNM にログインすると、DCNM はユーザーに LAN 資格情報の入力を求めます。前述のように、DCNM はこれらの資格情報を使用して、デバイスへの書き込みアクセス権を提供します。すべてのユーザーは、このプロセスに従う必要があります。社内のビジネス ポリシーにより、ユーザーは 3 ～ 6 か月ごとにパスワードを変更する必要があるとします。次に、すべてのユーザーは、DCNM **[LAN 資格情報（LAN Credentials）]** ウィンドウでデバイスにアクセスするためのパスワードを更新する必要があります。また、AAA サーバーでパスワードを更新する必要があります。

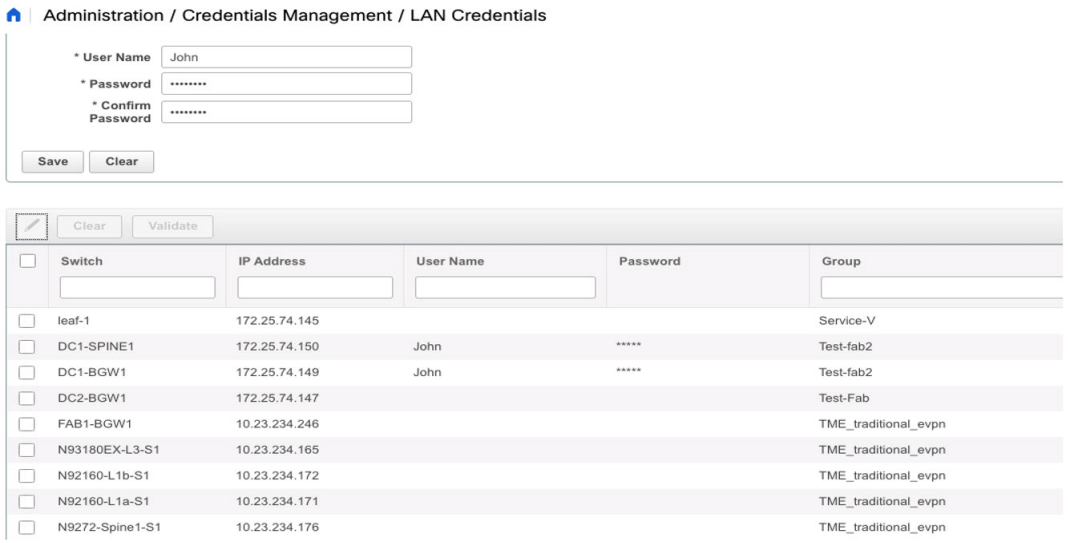
たとえば、ISE サーバーで認証を行う John という名前のユーザーについて考えてみましょう。

1. John は、自分のユーザー資格情報を使用して DCNM にログインします。
2. ISE サーバーは John のユーザー資格情報を認証し、DCNM は彼の LAN スイッチ資格情報を入力するためのメッセージを表示します。DCNM はこれらの資格情報を使用して、デバイスでさまざまな構成と書き込み操作を実行します。

3. John は、LAN スイッチの資格情報を入力します。DCNM は、すべてのデバイスで John によってトリガされるすべての書き込み操作に LAN スイッチ資格情報を使用します。ただし、John は、デバイスごとのアクセス ベースで LAN スイッチの資格情報を入力することを選択することもできます。このデバイスごとのアクセス オプションは、デフォルトの資格情報を入力することによって提供されるアクセスを上書きします。



John が再び DCNM にログインすると、DCNM は LAN スイッチ資格情報をすでにキャプチャしているため、LAN スイッチ資格情報を入力するためのメッセージを表示しません。John は、同じ資格情報を使用して、DCNM およびアクセス可能なデバイスにログインします。



4. ここで、数か月後に企業のITポリシーが変更されたとします。次に、Johnはリモート AAA サーバーで自分のパスワードを更新する必要があります。また、ステップ 3 を実行して、DCNM が LAN スイッチ資格情報を更新できるようにする必要があります。

したがって、このモードでは John が更新されたパスワードを使用して DCNM Web GUI にログインすると、DCNM は LAN 資格情報を入力するためのメッセージを表示しません。ただし、John は LAN 資格情報のパスワードを更新する必要があります。DCNM が新しく更新されたパスワードを継承し、デバイスで書き込み操作を実行できるようになるため、パスワードを更新する必要があります。

AAA リモート認証パススルー メカニズム

このモードでは、ユーザーがユーザー名とパスワードを入力して DCNM にログインすると、DCNM はそのユーザー資格情報をそのユーザーの LAN スイッチ資格情報設定のデフォルト資格情報に自動的にコピーします。その結果、ユーザーが初めてログインしたときに、DCNMは LAN スイッチ資格情報を入力するためのメッセージを表示しません。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。
2. `/root/directory`（**su** コマンドを使用）にログインします。
3. `/usr/local/cisco/dcm/fm/conf/server.properties` ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   dcnm.lanSwitch.sameUserAccount=true

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功すると、DCNM は LAN スイッチ資格情報を更新するためのメッセージを表示しません。これは、この情報がLANスイッチ資格情報に自動的にコピーされるためです。
8. 数か月後、企業の IT ポリシーが変更されることを考慮してください。このモードでは、John はリモート AAA サーバーでパスワードを更新する必要があります。その後、John が DCNM にログインすると、DCNM は更新された資格情報をユーザー John に関連付けられたデフォルトの LAN 資格情報に自動的にコピーします。

DCNM サービス アカウントを使用した AAA リモート認証

多くの場合、顧客は、共通のサービス アカウントを使用して DCNM コントローラから行われたすべての変更を追跡することを好みます。次の例では、ユーザーが DCNM コントローラを使用して変更を行い、デバイスに変更を加えています。これらの変更は、共通のサービスアカウントに対してデバイス上で監査ログに記録されます。したがって、コントローラによってトリガされた変更を、ユーザーがデバイス上で直接行った他の変更（アウトオブバンド変更とも呼ばれます）と区別することができます。アウトオブバンドの変更は、ユーザーアカウントから行われたデバイス アカウンティング ログに表示されます。

たとえば、リモート AAA サーバーに**ロボット**という名前のサービス アカウントを作成します。対応する資格情報を使用して、ロボット ユーザーは DCNM にログインできます。ロボット ユーザーは、デフォルトの LAN 資格情報を入力して、デバイスへの書き込みアクセス権を持つことができます。DCNM network-admin は、すべてのユーザーのデフォルトの LAN 資格情報を自動的に設定し、ロボットに関連付けられたデフォルトの LAN クレデンシャルを継承するサーバー プロパティを有効にします。

したがって、ユーザーが DCNM にログインして構成を変更すると、DCNM はロボットの LAN 資格情報を使用して変更をデバイスにプッシュします。DCNM 展開履歴ログは、変更をトリガしたユーザーを追跡し、DCNM からスイッチに展開された対応する変更をユーザー ロボットの監査ログで表示します。

DCNM でサービス アカウントを設定するには、次の手順を実行します。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。
2. `/root/ directory`（**su** コマンドを使用）にログインします。
3. `/usr/local/cisco/dcm/fm/conf/server.properties` ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   service.account=robot

（注） AAA パススルー アカウントまたはサービス アカウントのいずれかを有効にできます。

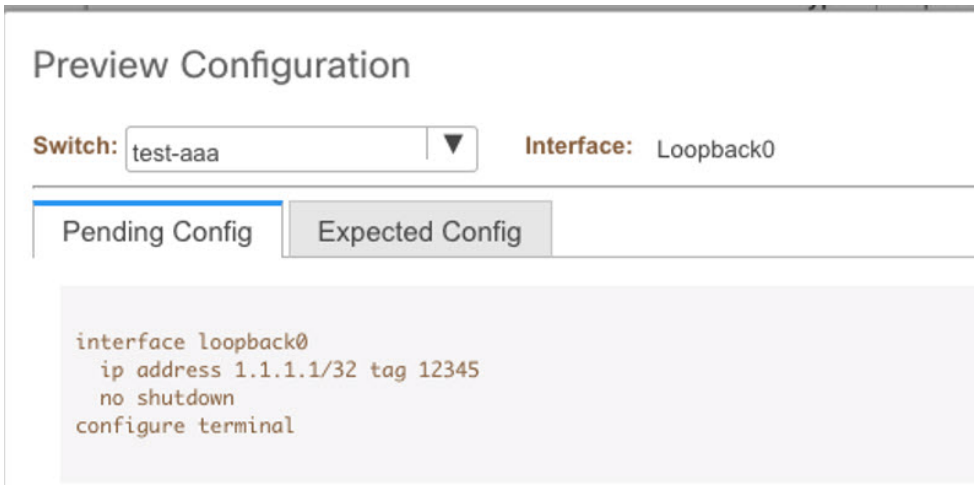
```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功した後、DCNM は LAN スイッチ資格情報を更新するためのメッセージを表示しません。ただし、John が **[LAN 資格情報（LAN Credentials）]** ページに移動すると、DCNM は、サービス アカウントが DCNM で有効になっているため、すべての LAN 資格情報がサービス アカウントから継承されることを示すメッセージを表示します。

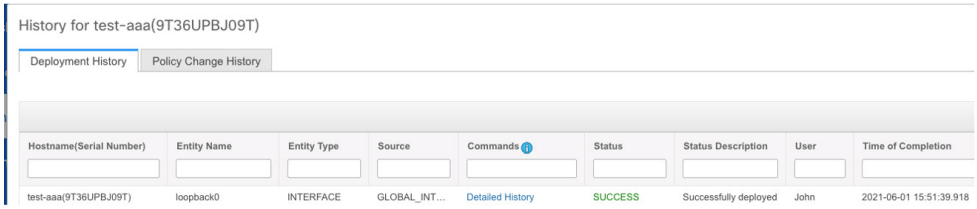
サービス アカウント構成監査

次のワークフローの例では、DCNM サービスアカウント機能の使用中に構成監査を検証できます。ただし、サービスアカウントのアクティブ化手順を完了している必要があります。

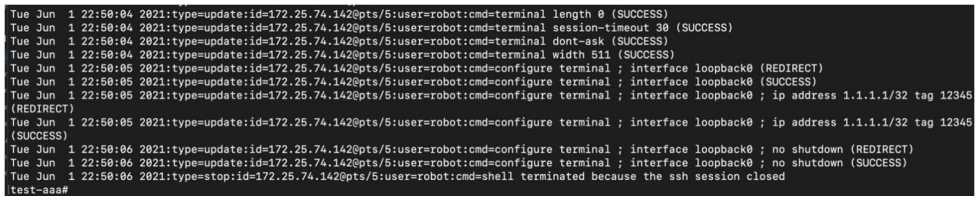
1. John は、デバイスでテスト ループバックを作成します。

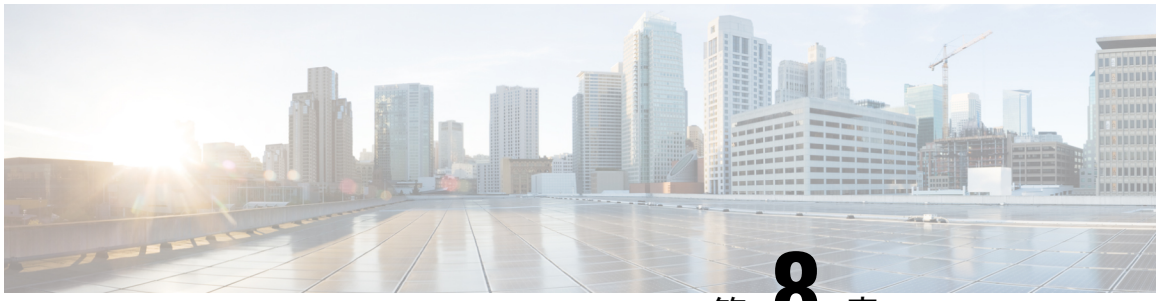


2. John は、DCNM を使用して構成を展開します。
3. DCNM 展開の履歴により、John が最近の構成変更を行ったことを確認できます。



4. デバイスのアカウンティングログは、DCNM サービスアカウント（つまり、この例ではロボット）が NX-OS デバイスの変更をトリガしたことを示しています。





第 8 章

[ServiceNow との DCNM 統合（DCNM Integration with ServiceNow）]

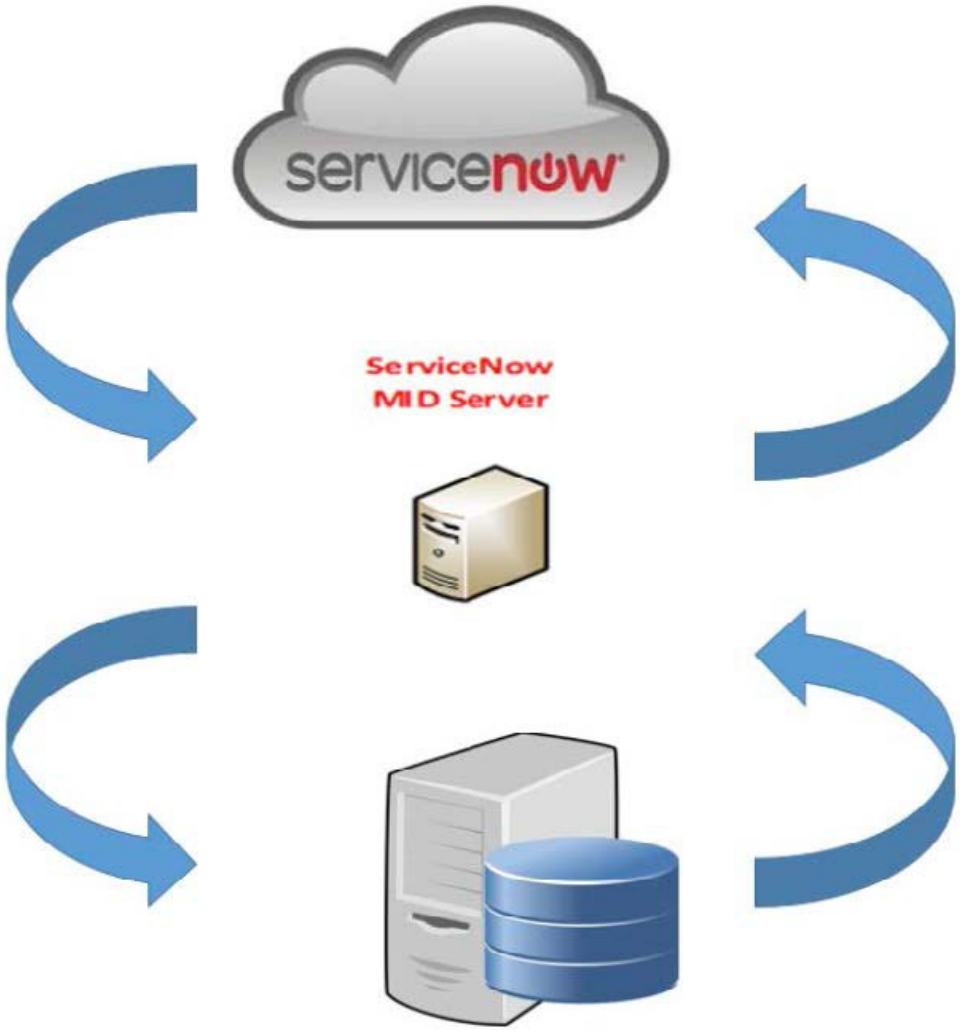
DCNM と ServiceNowの統合

ServiceNow では、IT サービス管理（ITSM）および IT 運用管理（ITOM）のアプリケーションを提供します。4 つの主要なモジュールがあります：インベントリ検出、インシデント管理、イベント管理、変更管理ワークフローです。Cisco DCNM リリース 11.3(1) 以降、Cisco DCNM と ServiceNow の統合を提供します。これにより、エンドユーザーの IT データを ServiceNow プラットフォームと統合できます。統合により、構成データが入力された ServiceNow カスタム テーブルのデフォルト セットが提供されます。

この機能を利用するには、ServiceNow カスタマー インスタンスに DCNM アプリケーションをインストールし、DCNM ミッドサーバの詳細を提供します。スイッチの詳細、ポートの詳細、アラームに関する情報またはデータは、ServiceNow 構成管理データベース（CMDB）テーブルに取得されます。デフォルトでは、データは 15 分ごとに取得され、表示されます。

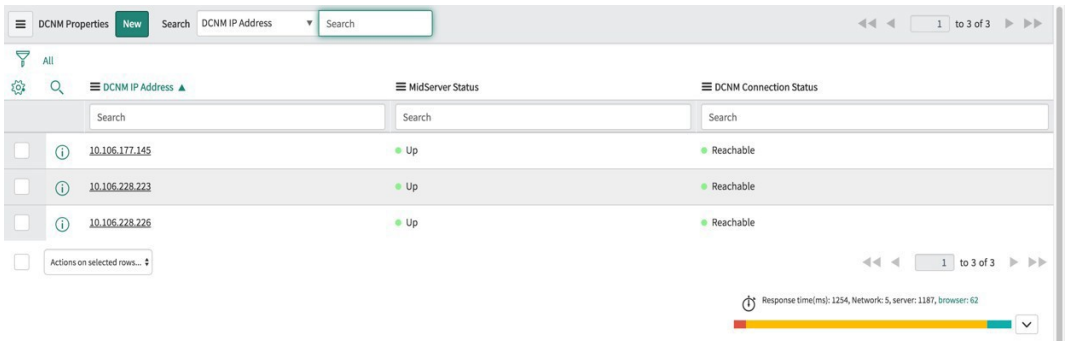
スイッチおよび各スイッチのポートに関する詳細は、DCNMインベントリから収集されます。アラームは、DCNMをポーリングすることによって収集されます。次に、アラームはフィルタリングされ、CPU、MEMORY、POWER、LINKSTATE、EXTERNAL、ICMP、SNMP、SSH などのタイプに基づいて分類されます。その後、アラームはイベントテーブルに保存されます。これらのイベントは、CPU、MEMORY、SNMP、および SSH カテゴリのインシデントを生成するために使用されます。各アラームのソース、説明、重大度、およびカテゴリが保存されます。ただし、アラームが DCNM に存在しなくなると、アラームに対して発生したインシデントは DCNM ServiceNow アプリケーションで更新またはクリアされません。アラームのポーリングが初めて開始されると、過去 7 日間に発生したアラームが DCNM から取り込まれます。

ServiceNow 上の DCNM アプリケーションは、スケジュールされたスクリプトを実行し、中間サーバに接続します。中間サーバは DCNM に接続してデータを取得します。DCNM は、要求されたデータを中間サーバに送信します。中間サーバは、そのデータを ServiceNow 上の DCNM アプリケーションに渡します。ServiceNow の DCNM インスタンスのテーブルには、この取得したデータが読み込まれます。



ServiceNow との DCNM 統合の注意事項と制限事項

- ServiceNow Cisco DCNM アプリケーション バージョン 1.0 では、1 つの MID サーバーに関する詳細のみを **[Cisco DCNM] > [プロパティ]** テーブルに追加できます。Cisco DCNM アプリケーション バージョン 1.1 以降、複数の MID サーバーを **[Cisco DCNM] > [プロパティ]** テーブルに追加できます。これは、複数の DCNM セットアップから同時にデータを取得できることを意味します。ServiceNow GUI では、各 DCNM からのデータは DCNM IP アドレスによって区別されます。

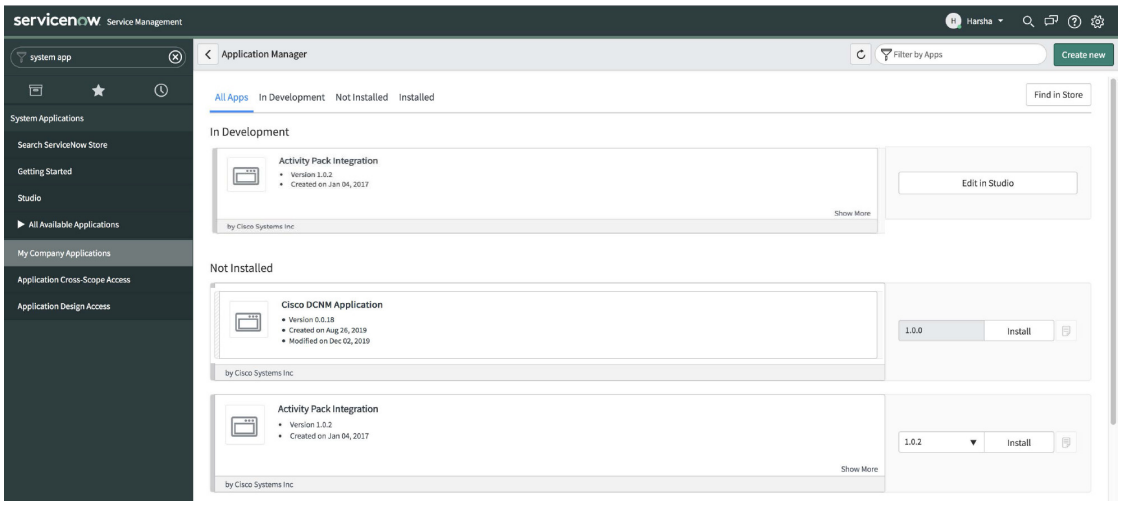


- データを取得するためにスケジュールされたスクリプトは、**[Cisco DCNM] > [プロパティ]** テーブルにサーバー レコードを挿入した後にのみ実行されます。
- **[Cisco DCNM] > [プロパティ]** テーブルの中間サーバーの IP アドレスとクレデンシャルが変更された場合、以前の中間サーバーを使用してインポートされたデータは、アプリケーション範囲テーブルから削除されます。ただし、ServiceNow CMDB（グローバル範囲）にインポートされたデータは残り、削除されません。
- ServiceNow データベースで最適なパフォーマンスを確保するために、各エントリはスイッチ データベース ID および IP アドレスと照合され、エントリが重複しないようにします。
- **[Cisco DCNM] > [プロパティ]** テーブルに新しいサーバーが追加された場合は、cmdb_ci_ip_switch テーブルのエントリを手動で削除する必要があります。

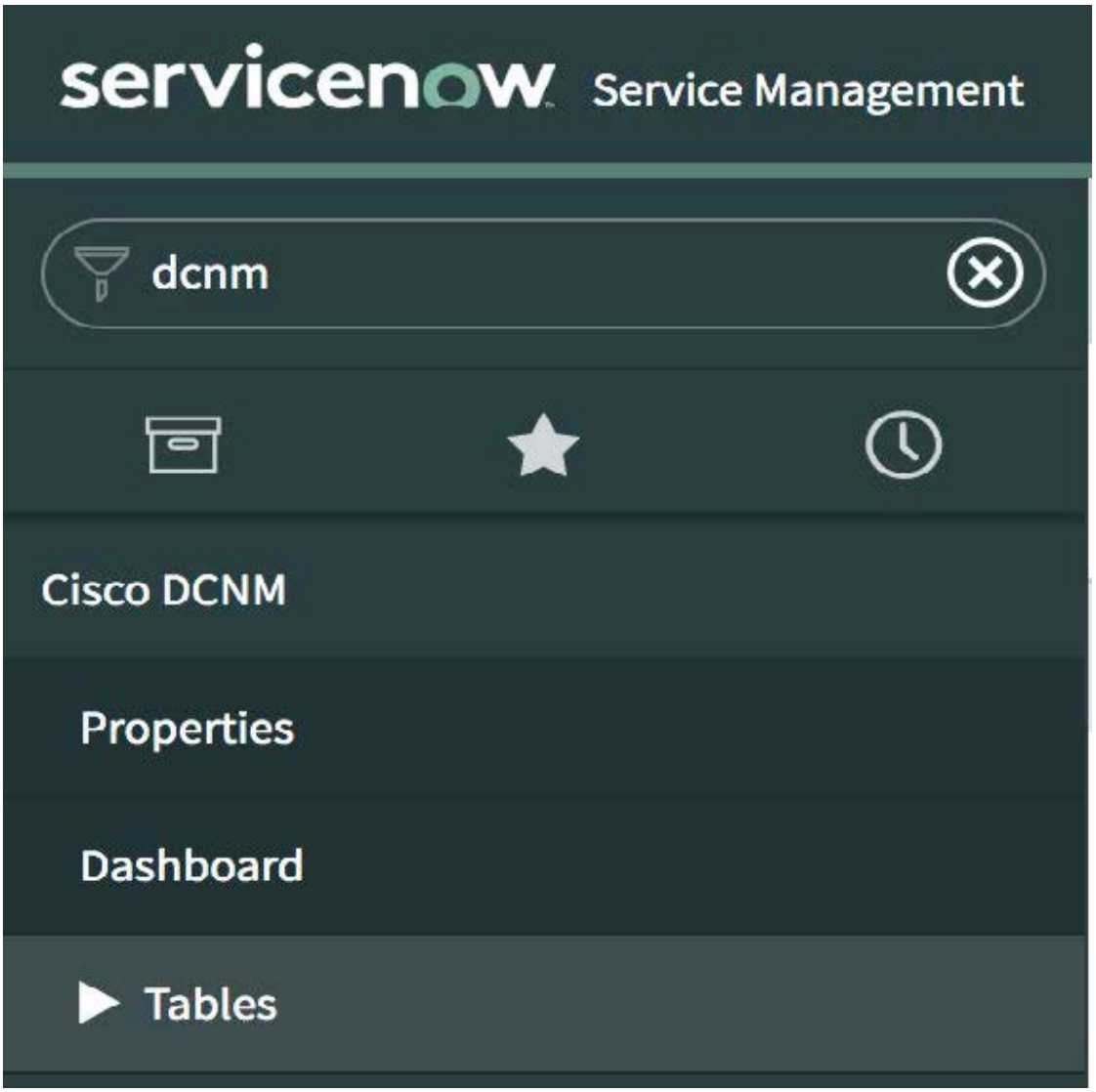
ServiceNow での Cisco DCNM アプリケーションのインストールと構成

Procedure

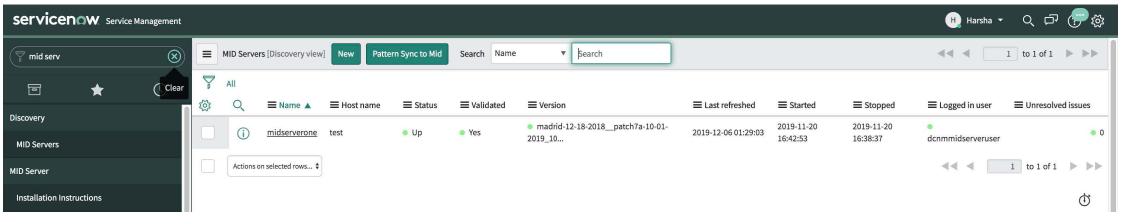
ステップ 1 https://dcnm1.service-now.com にログインします。**[システム アプリケーション（System Applications）] > [アプリケーション（Applications）]** を選択します。**[すべてのアプリケーション（All Apps）]** タブから **Cisco DCNM アプリケーション**をインストールします。



ステップ 2 インストールが完了したら、Cisco DCNM の [プロパティ（Properties）] タブと [ダッシュボード（Dashboard）] タブがアプリケーションに表示されていることを確認します。

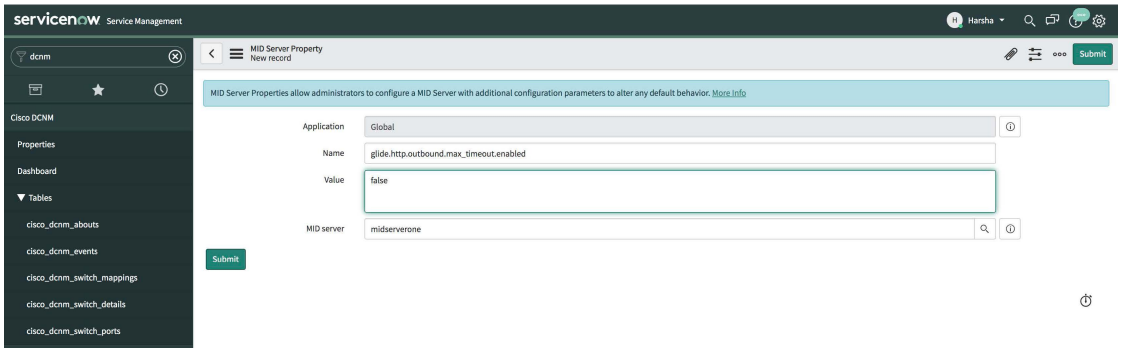


ステップ 3 **[中間サーバ（MID Servers）]** を選択し、DCNM 統合に使用される中間サーバをクリックします。

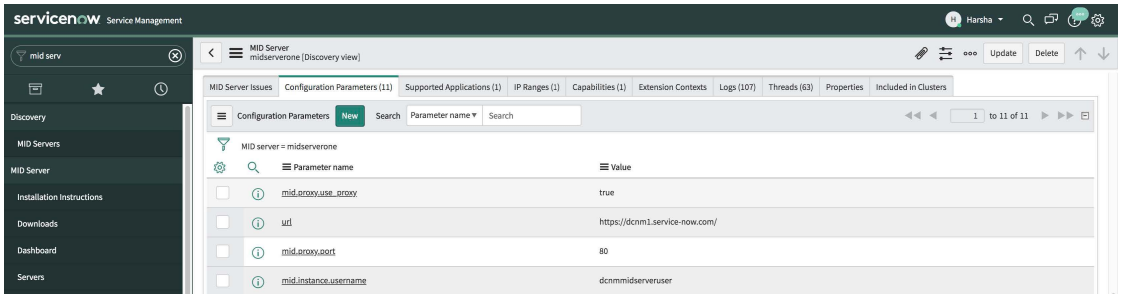


ステップ 4 下にスクロールして、**[プロパティ（Properties）]** タブをクリックします。**[新規（New）]** をクリックし、**[中間サーバ プロパティの新規レコード（MID Server Property New record）]** ウィンドウで以下に示すプロパティを追加します。[送信（Submit）] をクリックします。

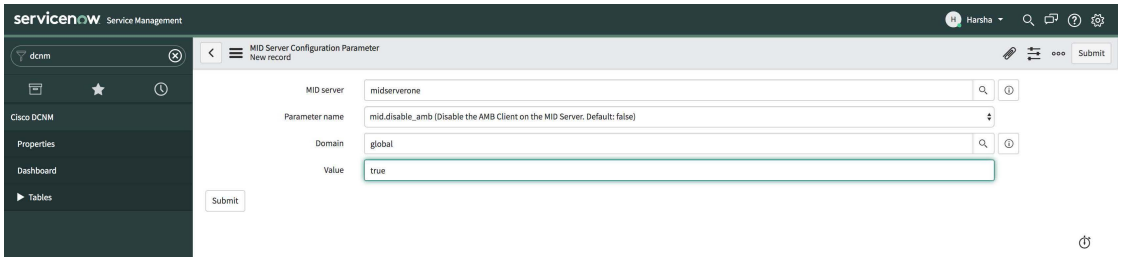
名前	[タイプ（Type）]	値
glide.http.outbound.max_timeout.enabled	True/false	False



ステップ 5　次に、**[構成パラメータ（Configuration Parameters）]** タブを選択します。

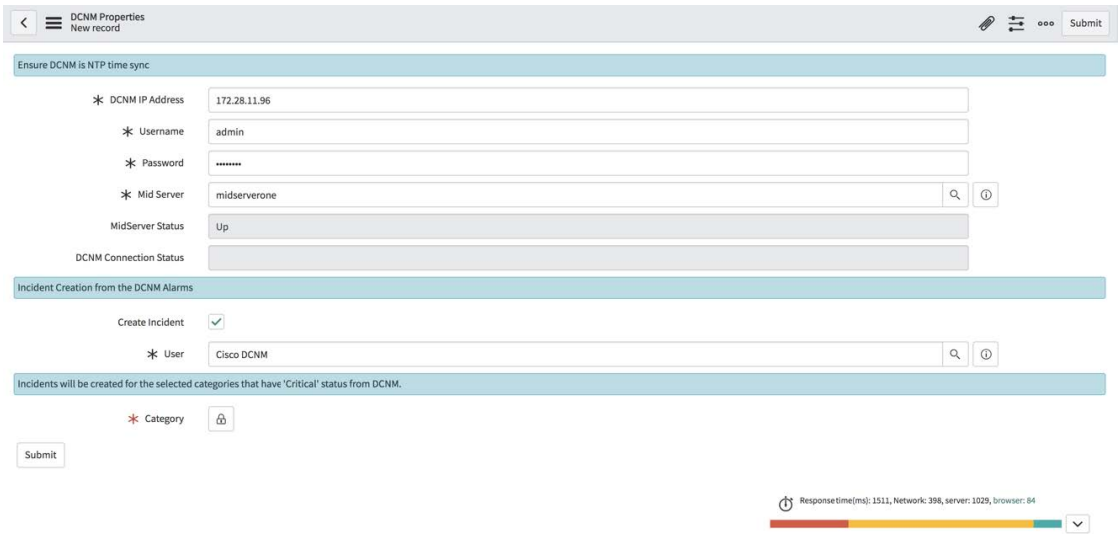


ステップ 6　**[構成パラメータ（Configuration Parameters）]** タブで、**[新規（New）]** をクリックします。フィールドに必要な詳細情報を入力します。



ステップ 7　**[送信（Submit）]** をクリックして中間サーバを設定します。

ステップ 8　**[Cisco DCNM] > [プロパティ（Properties）]** を選択します。**[新規サーバ（New Server）]** をクリックします。必須パラメータを入力します。



DCNM IP アドレス - DCNM の IP アドレス。

ユーザー名 - DCNM へのログインに使用するユーザー名を入力します。

パスワード - DCNM へのログインに使用するパスワードを入力します。

Note アクセス権は、DCNM 管理者のみに提供する必要があります。

中間サーバ - 使用する中間サーバの名前を指定します。名前は、入力時に自動的に入力されます。このフィールドの横にある検索アイコンをクリックして、[中間サーバ（MID Servers）] ウィンドウを表示することもできます。その後、表示されるリストから中間サーバを選択できます。

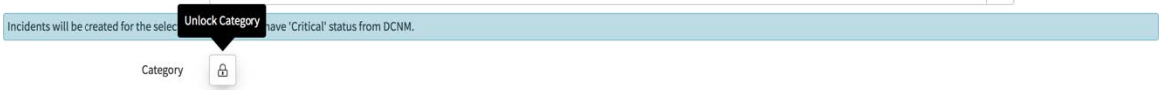
MidServer ステータス - 中間サーバが起動しているか、停止しているかを示します。

DCNM 接続ステータス - 提供された DCNM IP アドレスでデータを取得可能かできるかどうかを示します。このステータス フィールドは、必要な情報を入力した後に **[送信（Submit）]** をクリックすると入力されます。 DCNM との通信が成功した場合は **[到達可能（Reachable）]** が表示され、接続が失敗した場合は **[到達不能（Unreachable）]** と表示されます。

インシデントの作成 - アラーム イベントに対してインシデントを自動的に発生させる必要がある場合は、このチェックボックスを選択します。

ユーザー - 新しいユーザーを作成し、このフィールドにユーザー名を追加します。作成されたインシデントの [発信者（Caller）] フィールドには、このユーザー名が入力されます。このフィールドは、入力時に自動入力されます。このフィールドの横にある検索アイコンをクリックして、[ユーザー] ウィンドウを表示することもできます。表示されたリストからユーザーを選択できます。

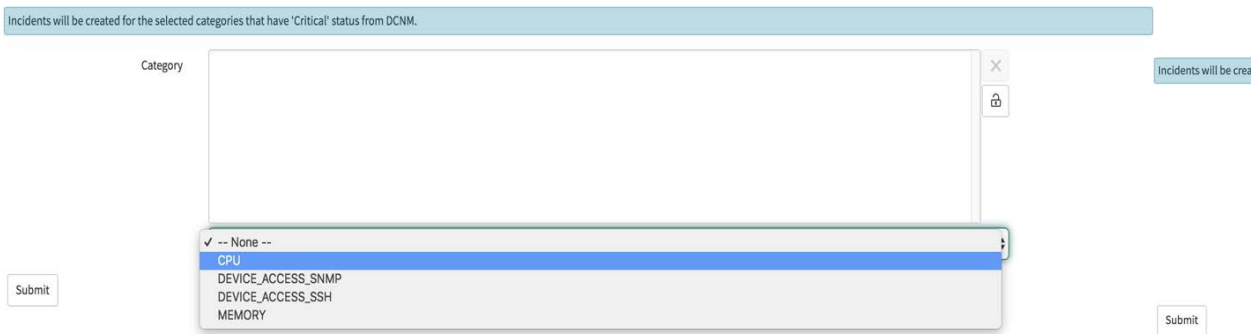
カテゴリ - ロック アイコン をクリックして、特定のカテゴリのみのインシデントを自動的に作成します。



[カテゴリ（Category）] ウィンドウの下にあるドロップダウンリストから、インシデントを作成する必要がある必要なカテゴリを選択します。インシデントの作成に使用できるカテゴリは、CPU、DEVICE_ACCESS_SNMP、DEVICE_ACCESS_SSH、および MEMORY です。詳細については、次の表を参照してください。

Table 32: イベントおよびインシデント

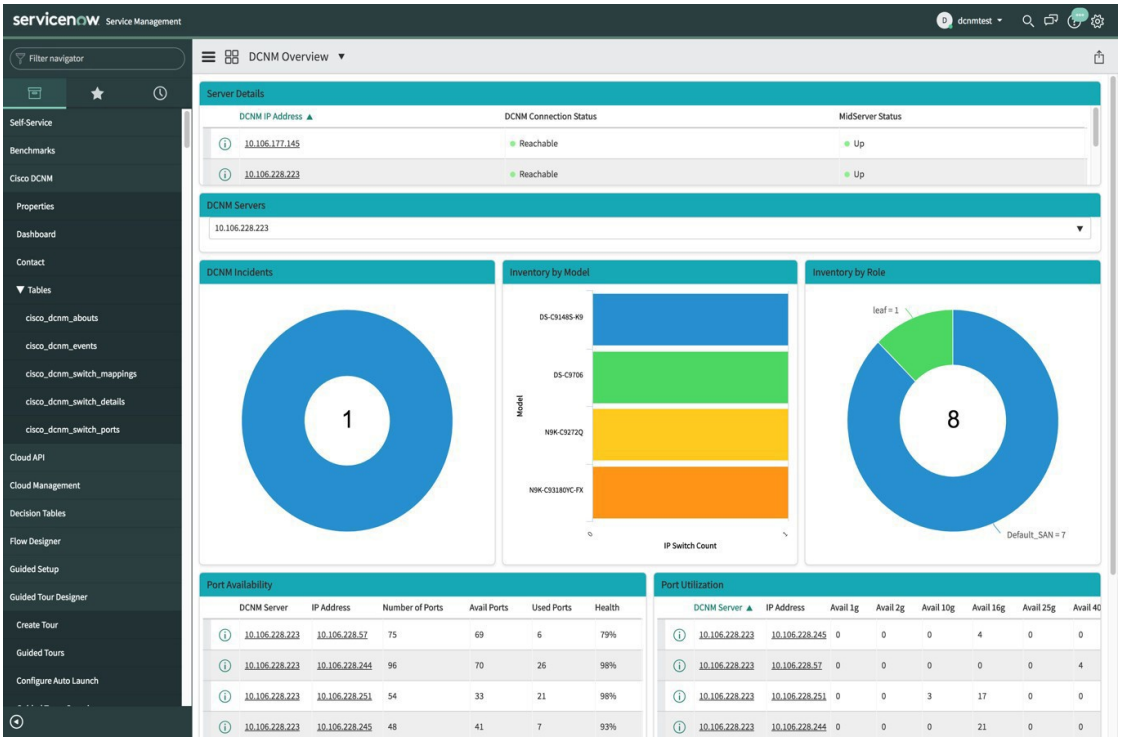
カテゴリ（**Category**）	**ServiceNow** でのデータ収集	発生したインシデント	インシデントルール	**ServiceNow** インシデントの詳細
CPU	はい	はい	DCNM アラームの重大度＝「重大」	優先順位＝2 緊急性＝2 影響度＝2
メモリ	はい	はい	DCNM アラームの重大度＝「重大」	優先順位＝2 緊急性＝2 影響度＝2
電源	はい	いいえ	該当なし	該当なし
Linkstate	はい	いいえ	該当なし	該当なし
ICMP	はい	いいえ	該当なし	該当なし
SNMP	はい	はい	DCNM アラームの重大度＝「重大」	優先順位＝2 緊急性＝2 影響度＝2
SSH	はい	はい	DCNM アラームの重大度＝「重大」	優先順位＝2 緊急性＝2 影響度＝2



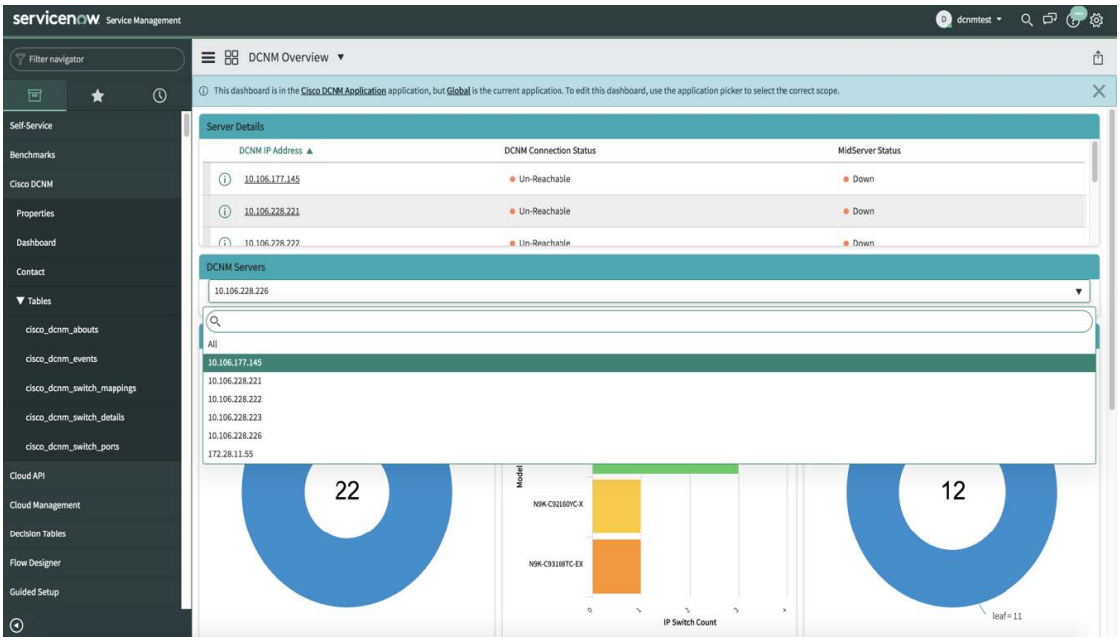
そして、**[Submit (送信)]** をクリックします。

ダッシュボードの表示

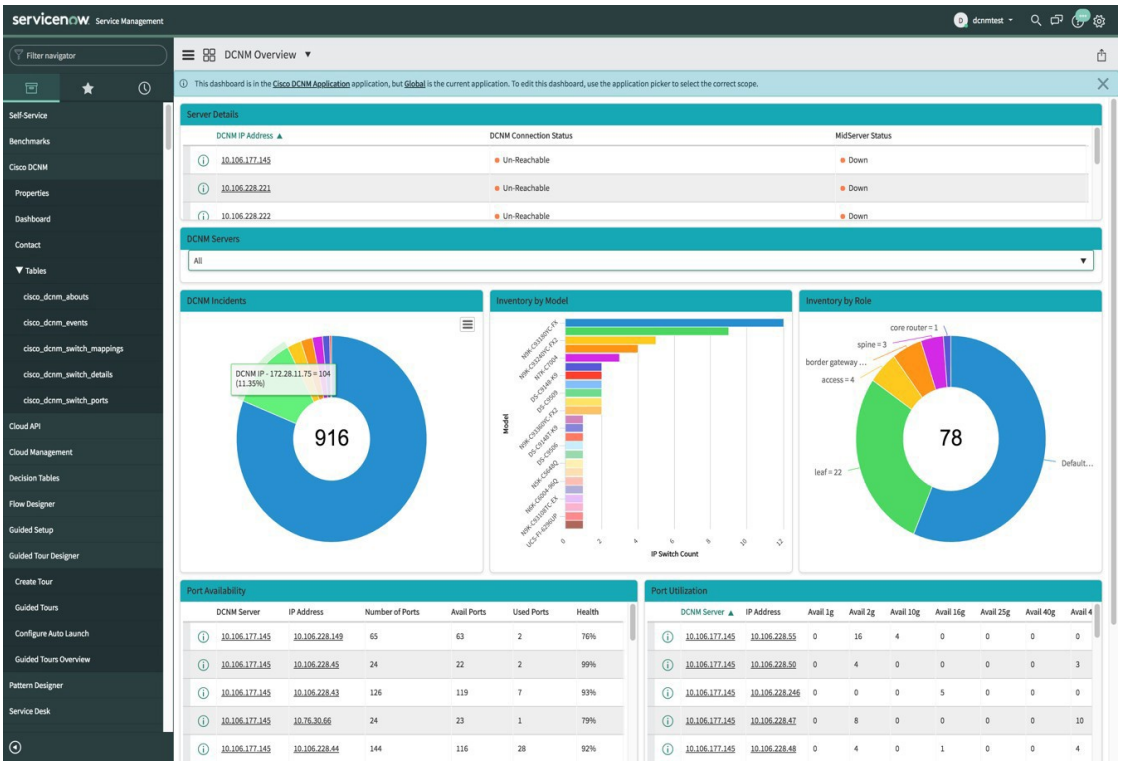
[Cisco DCNM] > [Dashboard（ダッシュボード）] を選択して、ダッシュボードを表示します。**DCNM IP アドレス**、**DCNM 接続ステータス**、および **MidServer ステータス**がダッシュボードの上部に表示されます。



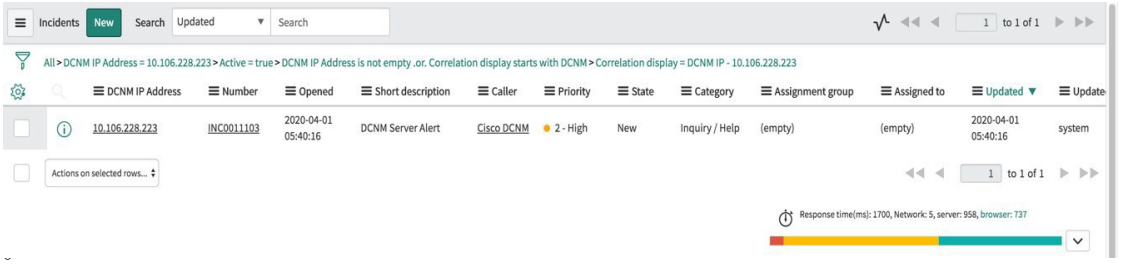
[DCNM サーバー] セクションには、データが取得および表示される DCNM サーバの IP アドレスが表示されます。ドロップダウン リストをクリックして、要件に応じて他の DCNM サーバを選択します。



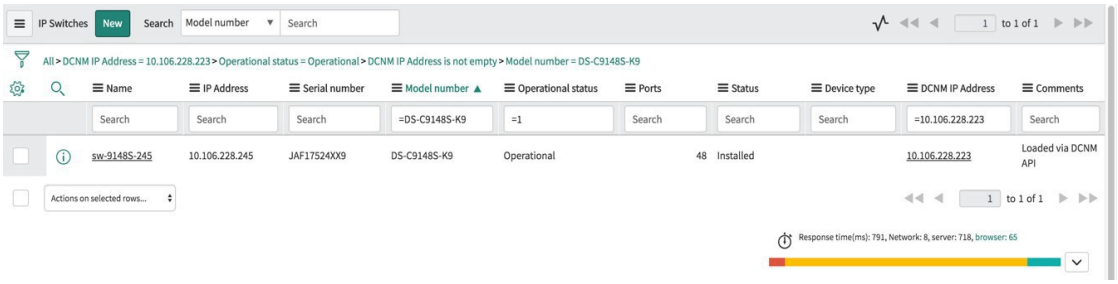
[すべて（All）] をクリックして、ドロップダウン リストに表示されているすべての DCNM サーバーからデータを取得して表示します。**[すべて]** オプションを選択すると、DCNM インシデント ドーナツに表示されるインシデントの数が色分けされ、さまざまな DCNM サーバーの IP アドレスに基づいて表示されます。[モデル別インベントリ（Inventory by Model）] ドーナツおよび [ロール別インベントリ（Inventory by Role）] ドーナツには、すべての DCNM サーバーからのデータも表示されます。ポートの可用性とポート使用率のドーナツには、各 IP アドレスが属する DCNM サーバーとともにデータが表示されます。



DCNM インシデント - これには、DCNM から取得したアラームに基づいて発生したインシデントの数が表示されます。インシデントの詳細については、ドーナツをクリックしてくださ

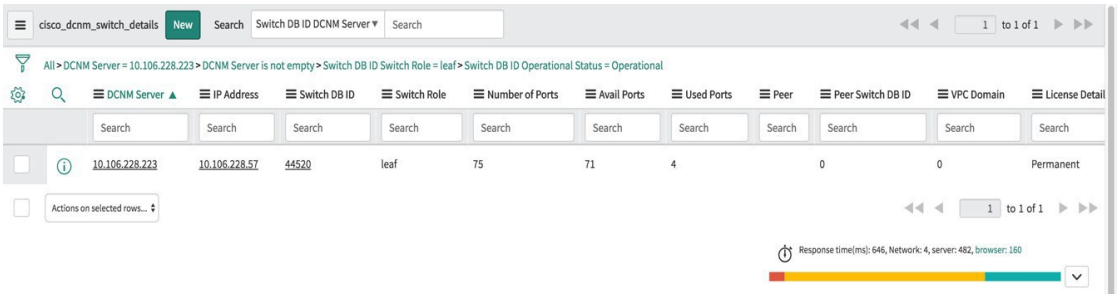


モデル別インベントリ - DCNM に存在するスイッチの数とタイプを表示します。各バンドはデバイス モデルを表します。詳細については、バンドをクリックしてください。

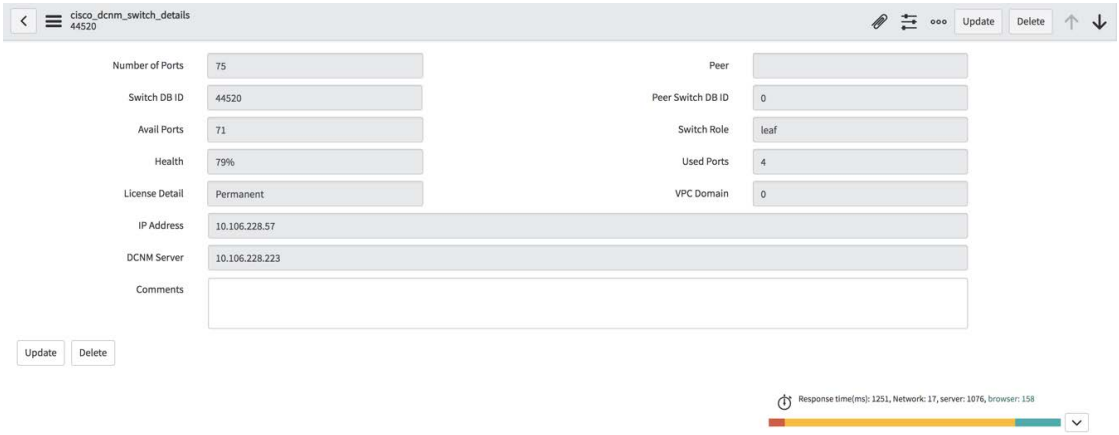


ロール別インベントリ - DCNM に存在するスイッチ ロールの数とタイプが表示されます。必要なセクションをクリックして、操作可能な役割の数を表示し、その絵図をクリックしてロールに関する詳細を表示します。

（注） [ロール別インベントリ] ドーナツに表示される数は、スイッチが DCNM から削除されても変わりません。削除されたスイッチは Non Operational として表示され、ドーナツに表示される番号に変更はありません。

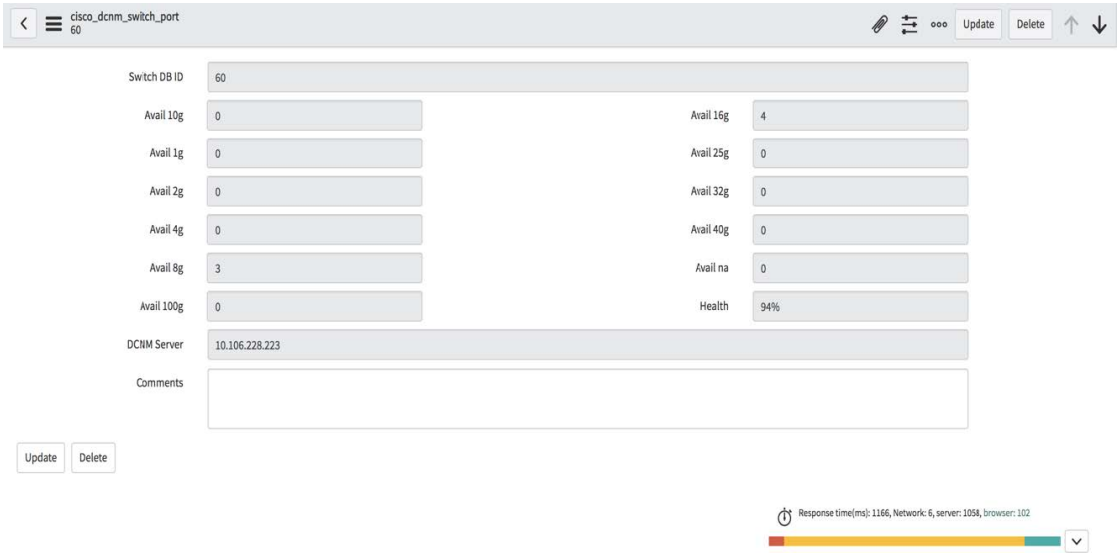


ポートの可用性 - ポートの可用性に関する情報が表示されます。ポートの総数、使用可能なポート、使用されているポート、およびスイッチのヘルスとともに、DCNM サーバーと IP アドレスが表示されます。IP アドレスをクリックすると、詳細が表示されます。



ポート使用率 - これは、各 IP アドレスに基づいたポート使用率に関する情報を表示します。1G、2G、4G、8G、10G、16G、25G、32G、40G、100Gのポート数が表示されます。IPアドレ

スをクリックすると、詳細が表示されます。



お問い合わせ

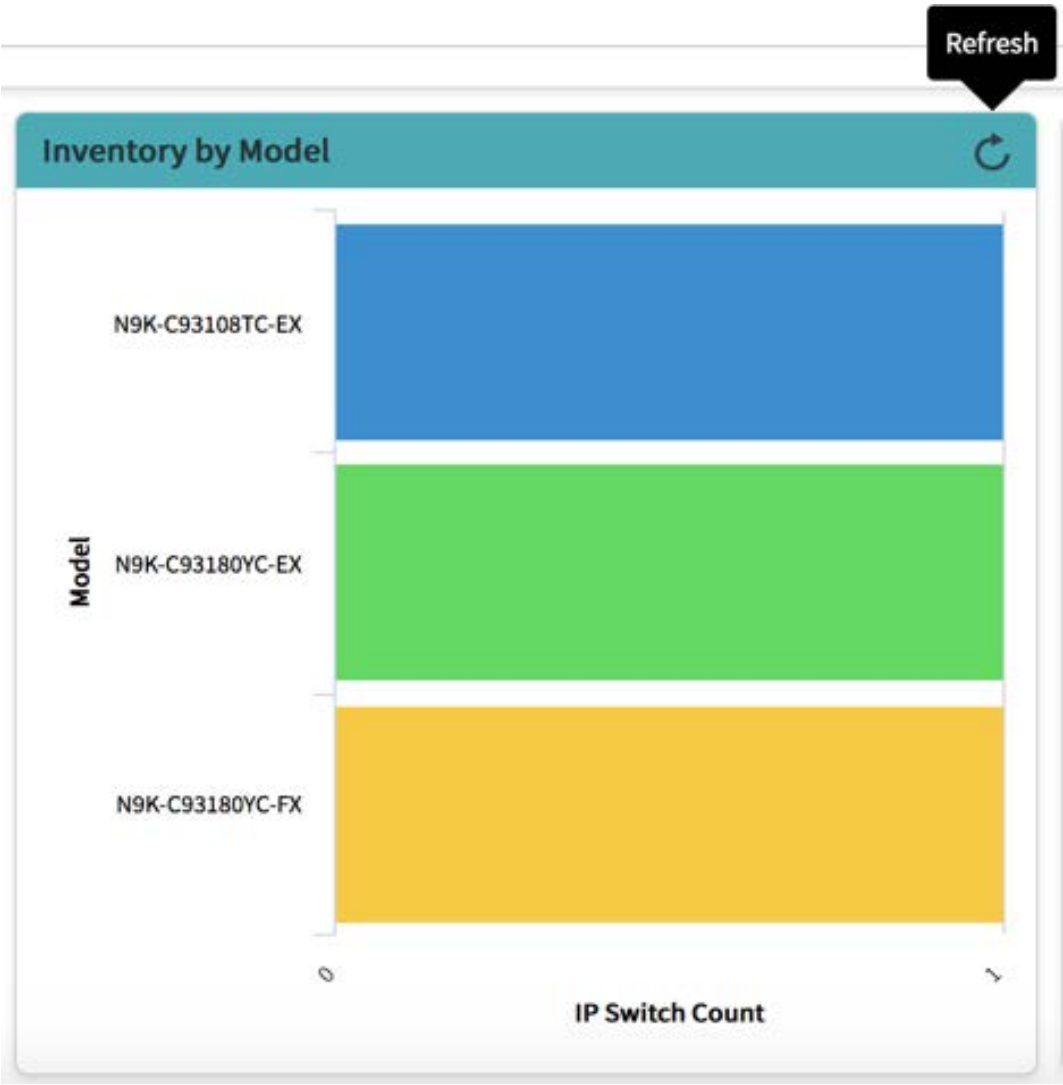
[Cisco DCNM] > [お問い合わせ（Contact）] を選択して、問い合わせについてシスコ システムズに連絡するために使用できる電子メール アドレスと電話番号を表示します。

ServiceNow との DCNM 統合のトラブルシューティング

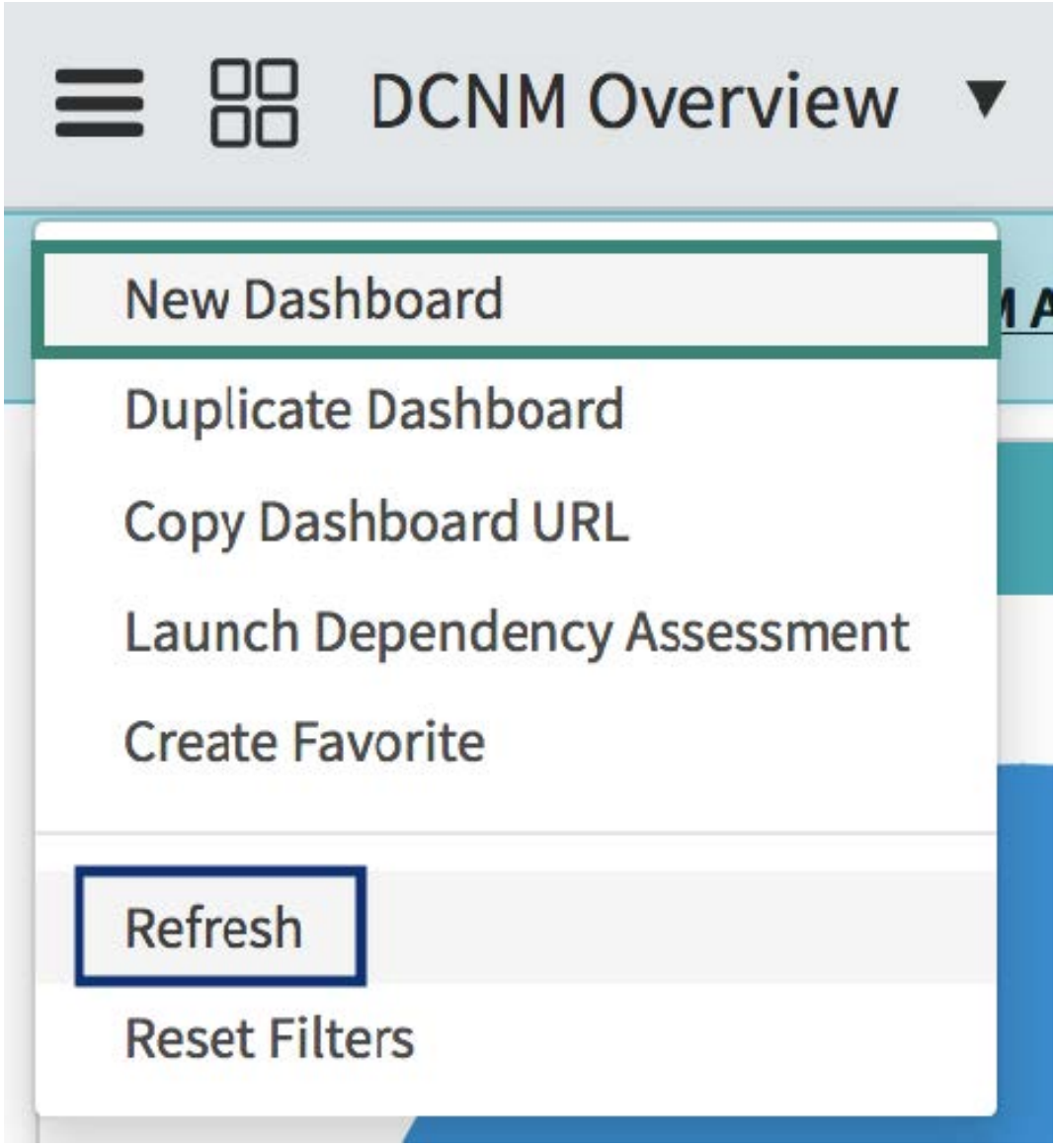
ServiceNow テーブルでデータが取得されていない場合：

- MID サーバーが起動しているか、停止しているかを確認します。
- 送信元「x_caci_cisco_dcnm」でシステム ログの情報エントリを確認します。
- Cisco DCNM プロパティに追加されたログイン情報を確認します。
- 選択した DCNM サーバーの ServiceNow ダッシュボードにデータが表示されていて、別の DCNM サーバーのデータを表示するシナリオを考えてみましょう。このようなシナリオでは、キャッシュの更新の遅延のため、ServiceNow ダッシュボードが他の DCNM サーバからデータを読み込むのに時間がかかることがあります。データを手動で更新するには、タ

イルの上にホバーしたときに個々のタイルの右上隅に表示される **[更新（Refresh）]** アイコンをクリックします。



[ダッシュボード コントロール（Dashboard Controls）] アイコンをクリックし、**[更新（Refresh）]** をクリックしてレポートを正しく読み込むことで、ダッシュボード全体を更新することもできます。



ServiceNow との DCNM アプリケーション統合の詳細については、ここをクリックしてください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。