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 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 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。

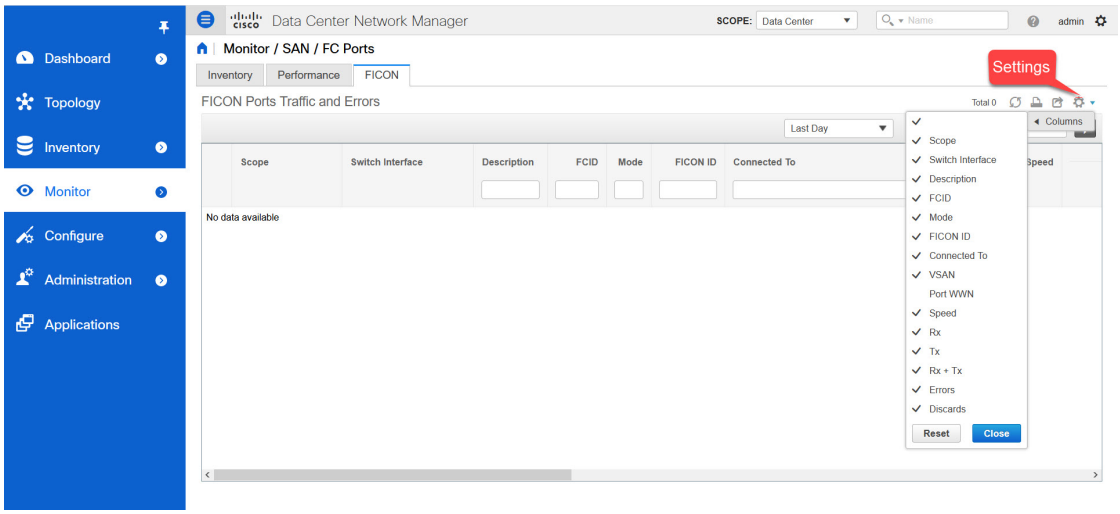
Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、セクション パフォーマンス セットアップのしきい値 を参照してください。

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 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 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 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 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 1: **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

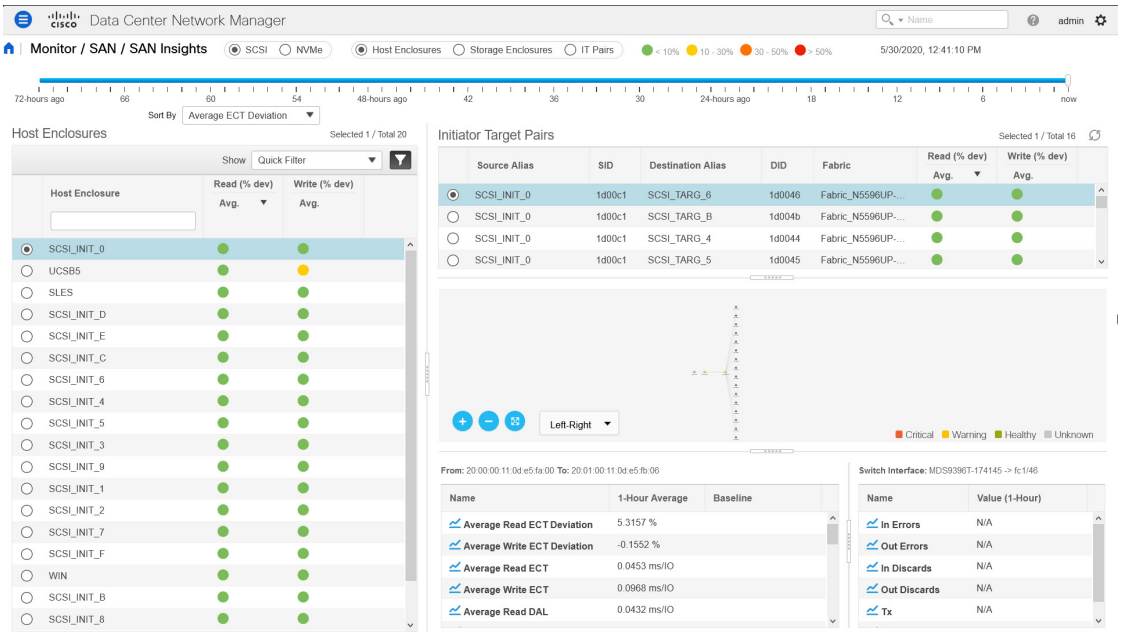
[SAN Insights（SAN Insights）] ページには、環境内の問題をすばやく特定できるように、インターフェイスにヘルス関連のインジケータが表示されます。ヘルスインジケータを使用して、ファブリックのどこに問題があるかを理解できます。

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。

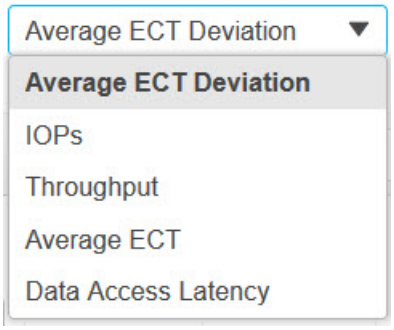
[モニタ（Monitor）] > [SAN Insights] ウィンドウでは、以下の手順で説明されているタスクを実行できます。

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。

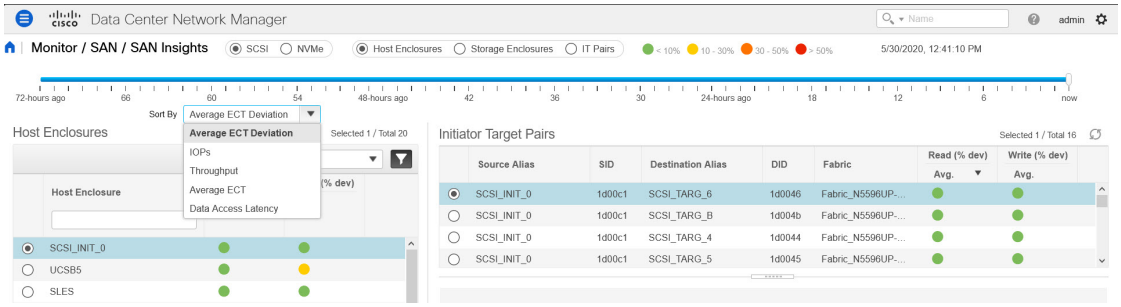
ステップ 2 **ホスト エンクロージャ、ストレージ エンクロージャ、**または**IT ペア**に関する詳細を表示します。

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。

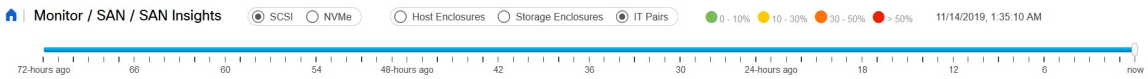


デフォルトでは、フィルタ タイプの **[平均 ECT 偏差]** が選択されています。イニシエータ ターゲット ペアには、読み取りおよび書き込み偏差のステータスが色付きのステータス ボールとして表示され、クリックして SAN Insights メトリックを表示できます。ただし、他のすべてのフィルタ タイプでは、読み取りおよび書き込みのパーセンテージ偏差のステータスが数値形式で表示されます。

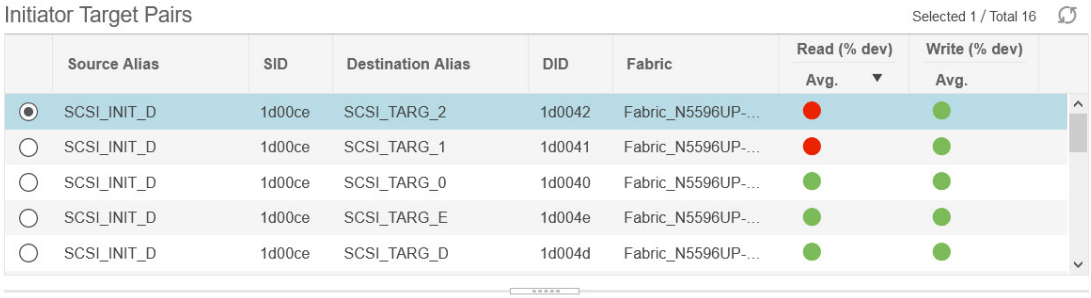
フィルタリングされたメトリックの読み取り/書き込み操作によって、エンクロージャ/IT ペアを並べ替えることができます。並べ替えを変更するには、列ヘッダをクリックします。デフォルトでは、読み取り操作でソートされています。



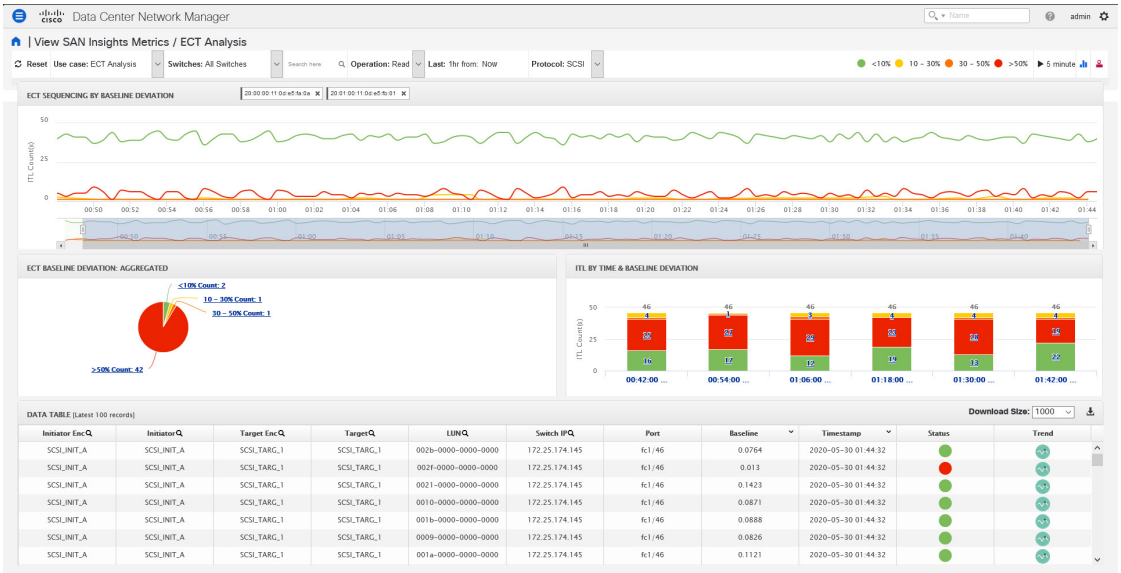
ステップ 3 時間間隔（現在、6時間前、12時間前など）を選択して、ステータスを計算し、フローとポートのカウンタを取得します。



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

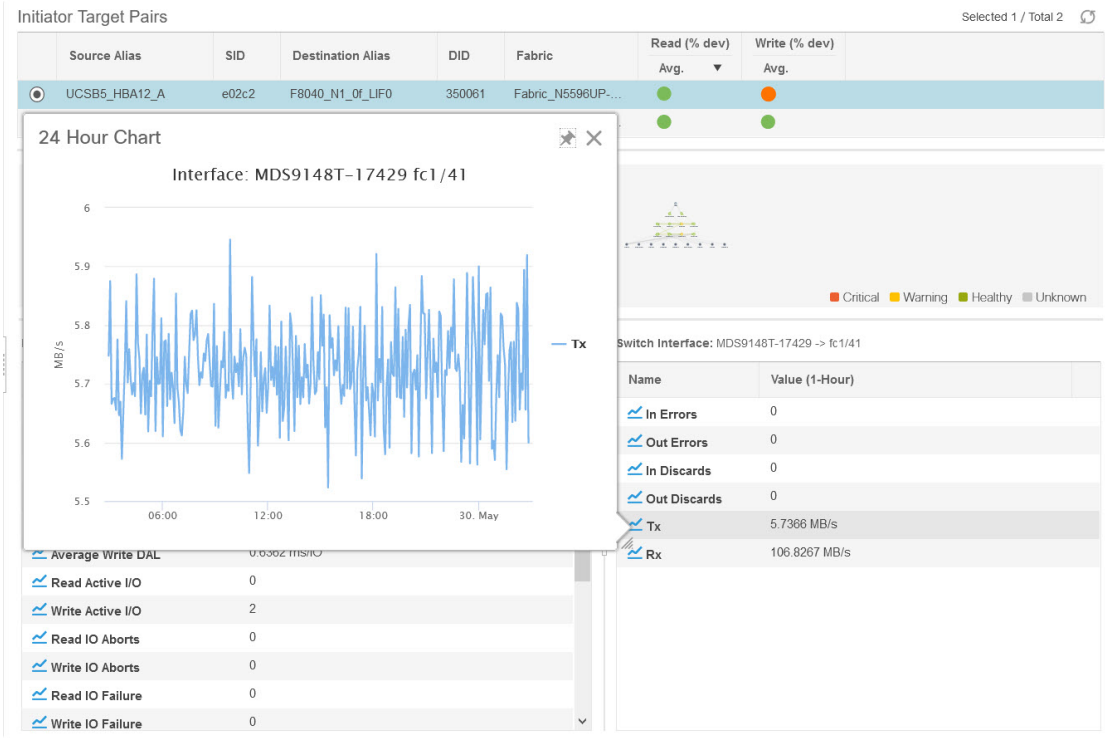
[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [SAN コレクション（SAN Collections）] を選択してパフォーマンス コレクションを有効にします。モニタするファブリックを選択します。ファブリックに対するすべてのパラメータ チェック ボックスをオンにします。**[適用（Apply）]** クリックして、パフォーマンスのモニタを開始します。

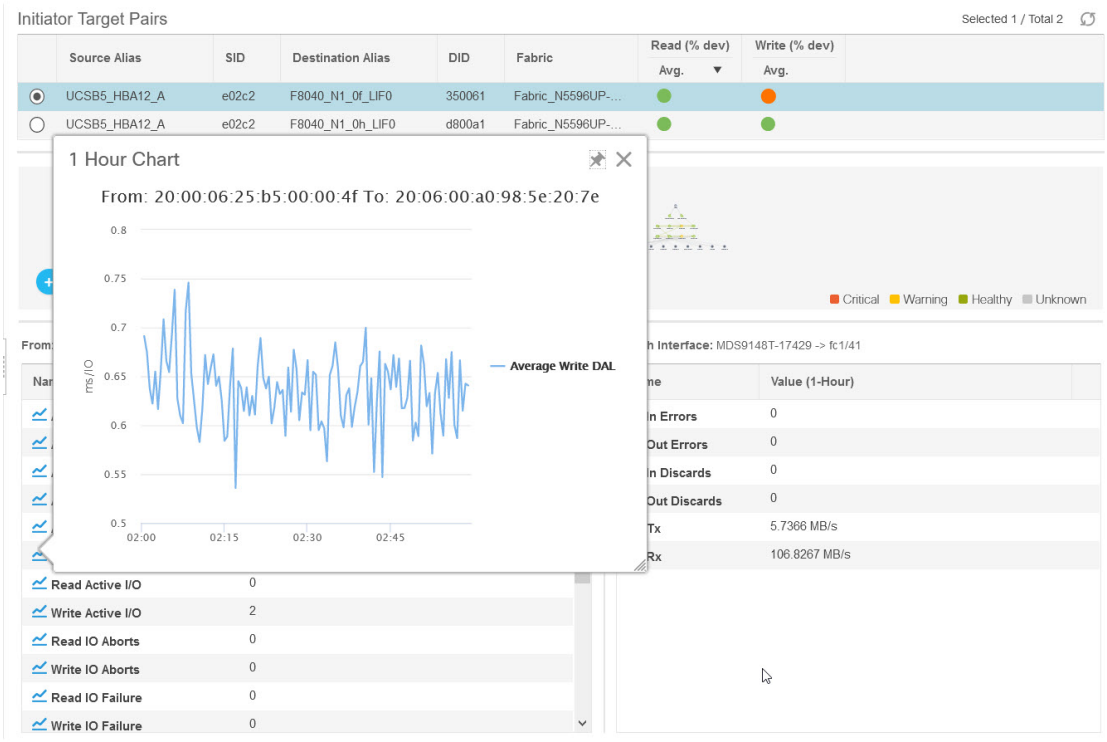
低速ドレイン メトリックを有効にするには、**[モニタ（Monitor）] > [SAN] > [低速ドレイン（Slow Drain Analysis）]** を選択します。ファブリックで現在のジョブを構成します。**[SAN Insights のモニタリング（Monitoring SAN Insights）]** で、マップ上のインターフェースをクリックします。**低速ドレイン メトリクス**は、スイッチ インターフェイス テーブルに表示されます。

- 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

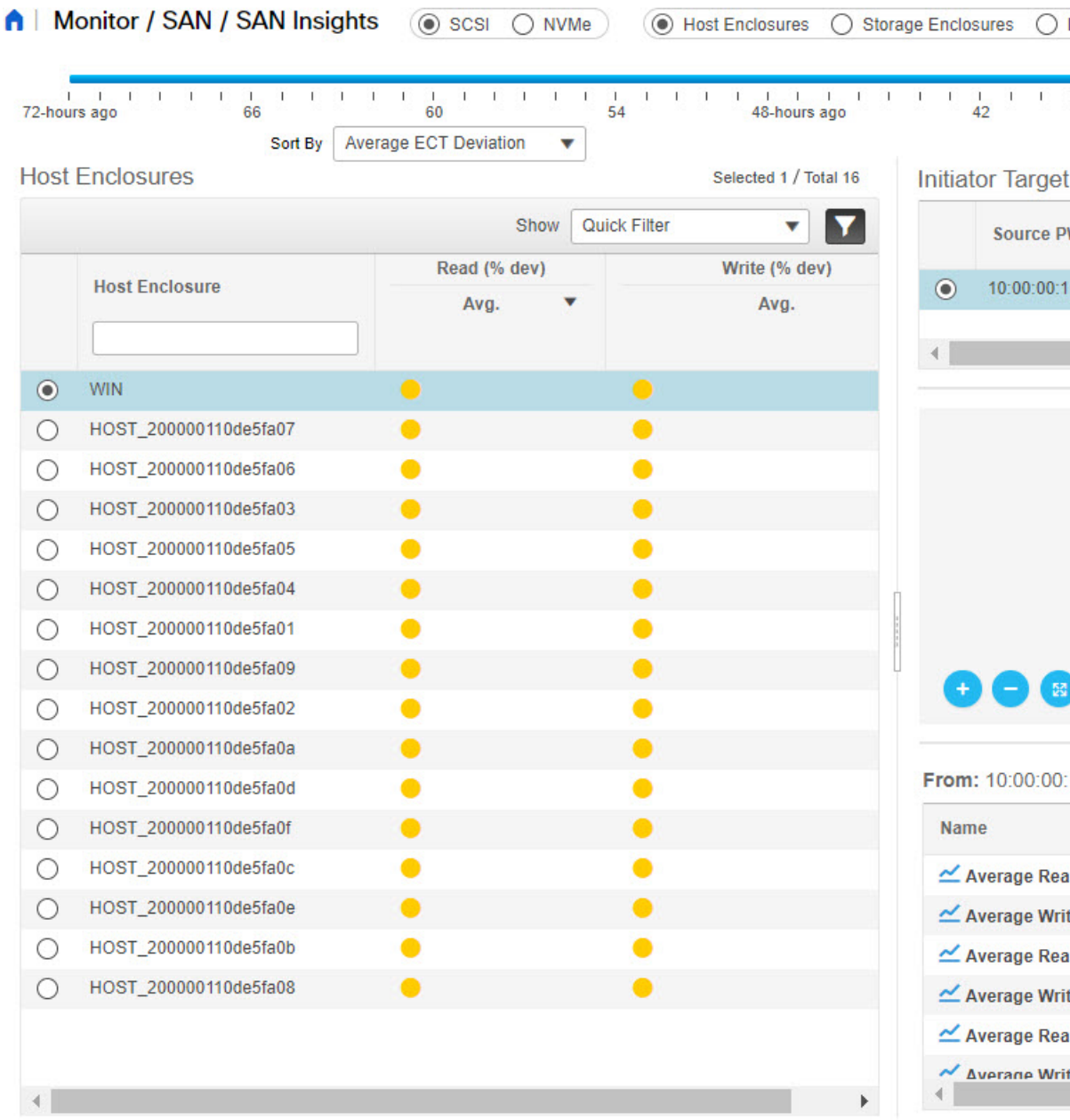

Initiator Target Pairs
Selected 1 / Total 2
Source Alias
SID
Destination Alias
DID
Fabric
Read (% dev)
Avg.
Write (% dev)
Avg.
UCSB5_HBA12_A
e02c2
F8040_N1_0f_LIF0
350061
Fabric_N5596UP-...
UCSB5_HBA12_A
e02c2
F8040_N1_0h_LIF0
d800a1
Fabric_N5596UP-...
1 Hour Chart
From: 20:00:06:25:b5:00:00:4f To: 20:06:00:a0:98:5e:20:7e
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。

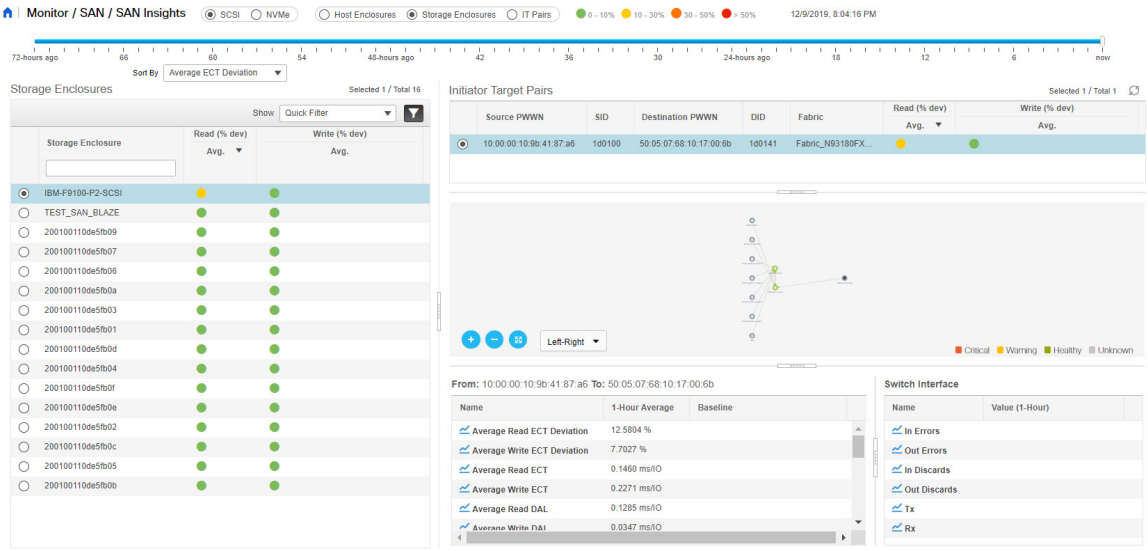
6. **[イニシエータ ターゲット ペア（Initiator Target Pairs）]** テーブルの **[読み取り (% dev)（Read (% dev)）]** または **[書き込み (% dev)（Write (% dev)）]** 列 にあるステータスの丸アイコンをクリックして、対応するイニシエータと事前にフィルタされたターゲット WWPN がある ECT 分析ウィンドウに移動します。

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。

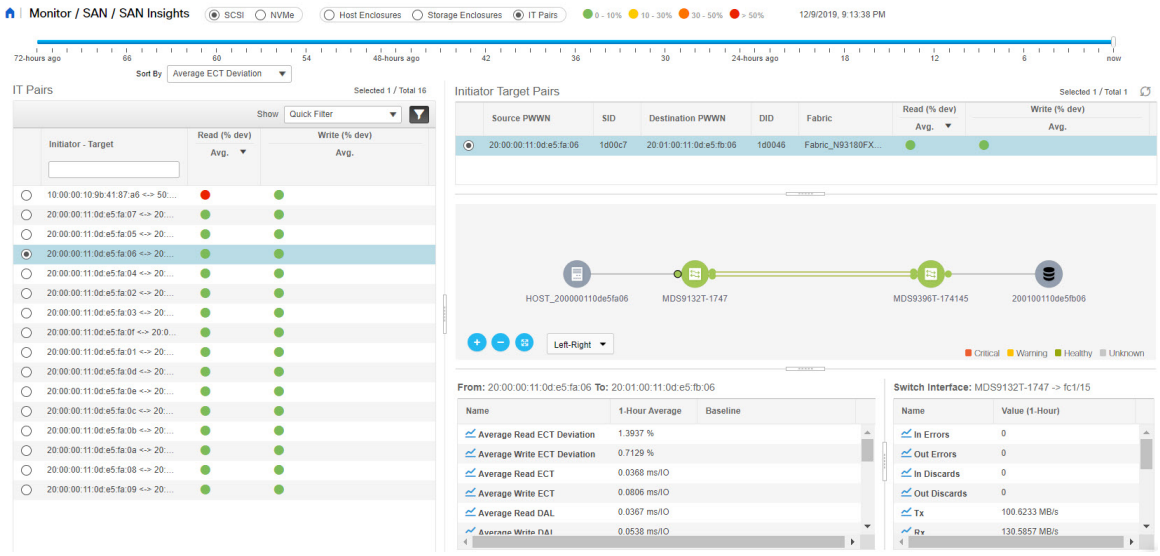
   [スイッチ インターフェイス（Switch Interface）] テーブルには、選択されたインターフェイスのデータが表示されます。リリース 11.4(1) から、スイッチ インターフェイスがピックアップされ、デフォルトで選択されます。

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 2: vPC パフォーマンス, on page 36 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 2: 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。

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。
- Performance Manager データの移行中に **[モニタ (Monitor)] > [アラーム (Alarms)] > [ポリシー (Policies)]** ウィンドウが開いていた場合、アラーム インデックスが削除される可能性があります。このようなシナリオでは、アラーム ポリシーが期待どおりに機能するように DCNM サーバーを再起動します。

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 3:* 例 *1

識別子	**ID1-ID2**
正規表現を上げる	ETHPORT-5-IF_ADMIN_UP：インターフェイス Ethernet15/1 で admin が起動されています。
正規表現のクリア	ETHPORT-5-IF_DOWN_NONE：インターフェイス Ethernet15/1 がダウンしています（トランシーバ欠落）

上記の例では、正規表現は端末モニタに表示される syslog メッセージの一部です。

Table 4:* 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 5: *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%

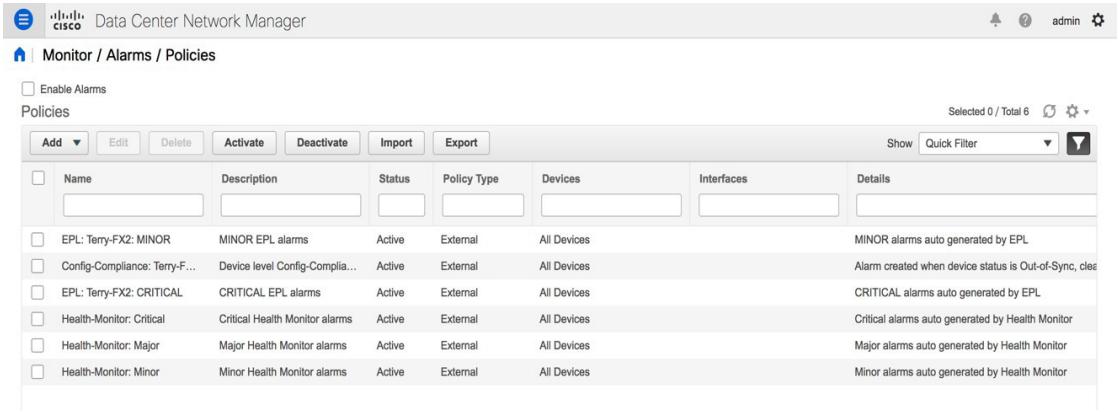
次のイベントの場合、アラームが発生し、メジャーとして分類されます。

- 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。

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。