モニター

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 （1 ページ）
- スイッチのモニタリング, on page 24
- LAN のモニタリング, on page 28
- エンドポイント ロケータ （34 ページ）
- アラーム, on page 34

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。

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 **[モニタ（Monitor）] > [インベントリ（Inventory）] > [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。

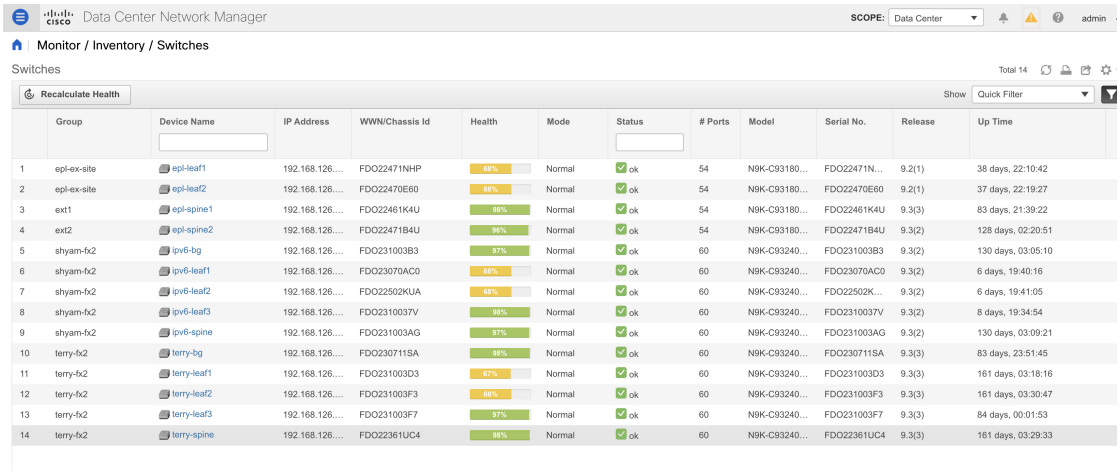
ステップ 2 次の情報が表示されます。

- **[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。

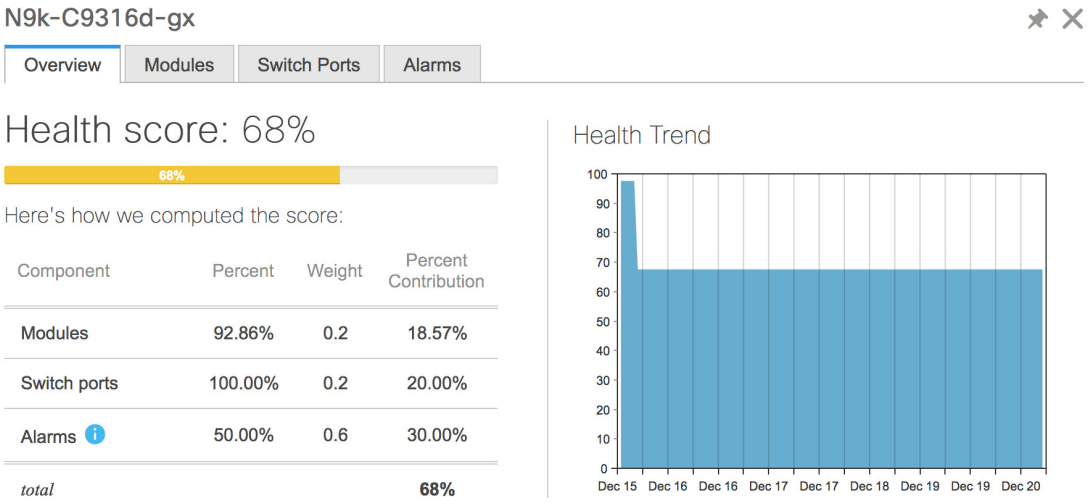
- **[ヘルス（Health）]** には、スイッチの正常性の状況が表示されます。

  Note Cisco DCNM 上のすべてのスイッチの最新のヘルス 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 **[ヘルスの再計算（Recalculate Health）]** ボタンをクリックします。

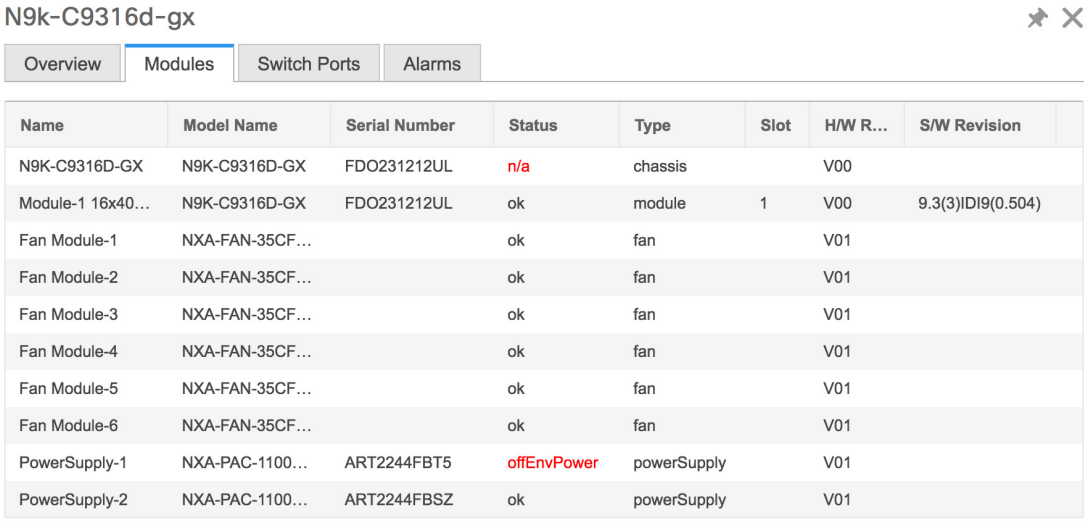
- **[モード]**列には、スイッチの現在のモードを指定します。スイッチは、**通常**、**メンテナンス**、または**移行**モードにすることができます。
- **[ステータス（Status）]** 列には、スイッチのステータスが表示されます。
- **[# ポート（#Ports）]** 列には、ポートの数が表示されます。
- **[モデル（Model）]** 列には、スイッチのモデル名が表示されます。
- **[シリアル番号（Serial No.）]** 列には、スイッチのシリアル番号を表示します。
- **[リリース（Release）]** 列には、スイッチのバージョンが表示されます。
- **[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。



ステップ 3 **[ヘルス（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。[ヘルス スコア（Health score）] ウィンドウには、ヘルス スコアの計算とヘルス トレンドが含まれています。[概要（Overview）] タブには、全体的なヘルス スコアが表示されます。ヘルス 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、[ヘルス 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。

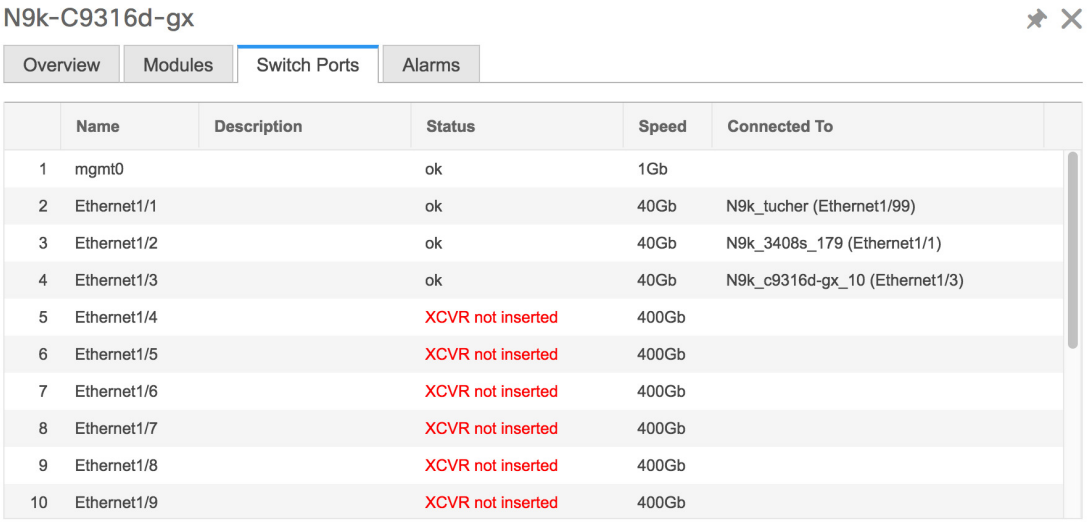


[モジュール]タブをクリックして、デバイスのさまざまなモジュールに関する情報を表示します。このタブには、名前、モデル名、シリアル番号、ステータス、タイプ、スロット、ハードウェア リビジョン、ソフトウェア リビジョンなどの情報が表示されます。

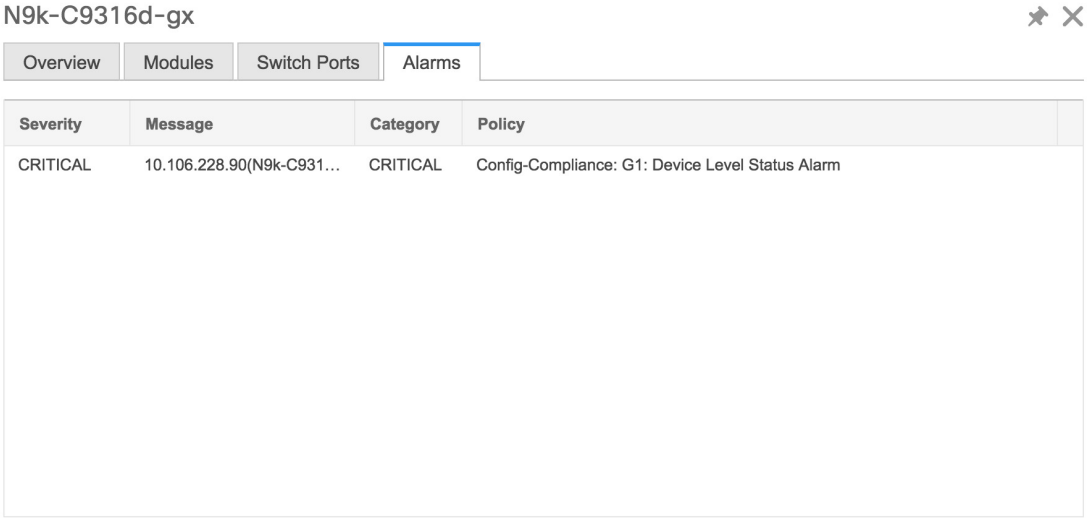


Name	Model Name	Serial Number	Status	Type	Slot	H/W R...	S/W Revision
N9K-C9316D-GX	N9K-C9316D-GX	FDO231212UL	n/a	chassis		V00	
Module-1 16x40...	N9K-C9316D-GX	FDO231212UL	ok	module	1	V00	9.3(3)IDI9(0.504)
Fan Module-1	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-2	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-3	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] 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。



[アラーム]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。



[ヘルス]列では、スイッチのヘルスは、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 **[ヘルス]** 列の値は、以下に基づいて計算されます。

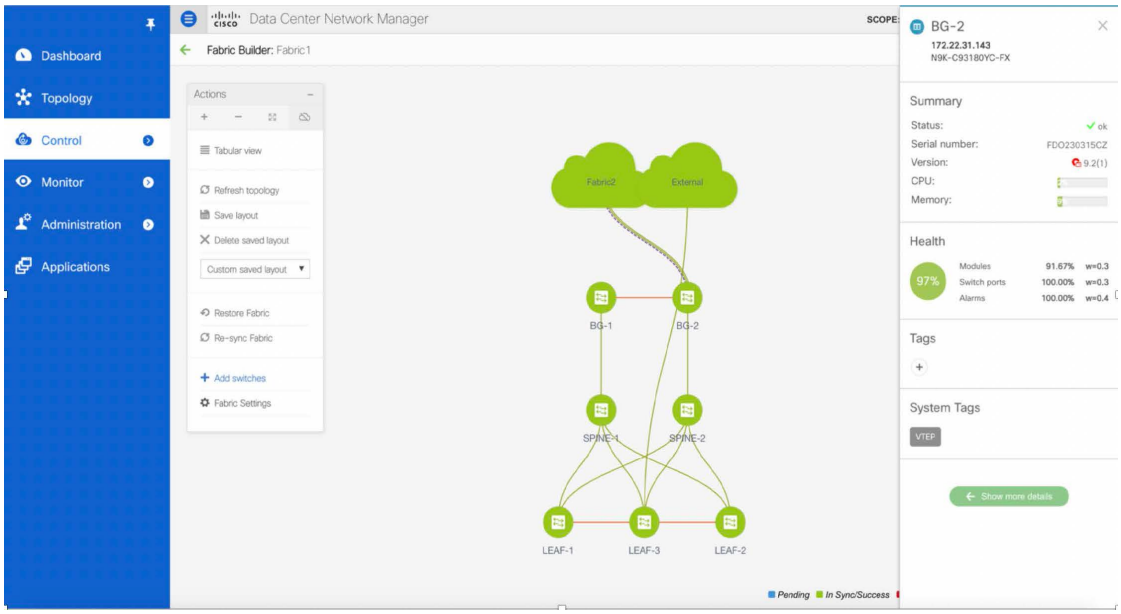
- 警告の影響を受けるモジュールの割合（正常性全体の 20% に寄与）。
- 警告の影響を受けるポートの割合（正常性全体の 20% に影響します）。
- アラームのパーセンテージ（正常性全体の 60% に影響します）。このパーセンテージの最大値を占めるのはクリティカル アラームで、次にメジャー アラーム、マイナー アラーム、および警告アラームが続きます。

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 スイッチのヘルスのみを計算します。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 [Unlicensed] をクリックします。[管理] > [ライセンス] 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、**[モニタ（Monitor）]>[インベントリ（Inventory）]>[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（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 **[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）**[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。

ホスト

スイッチのホストの詳細を表示できます。

[ホスト（Hosts）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[Device Name（デバイス名）]** 列でスイッチ名をクリックして、**[Hosts（ホスト）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *1*：ホスト タブ

フィールド	説明
VRF	スイッチの VRF 詳細を表示します。
ホスト IP	スイッチのホスト IP アドレスを表示します。
ホストのMACアドレス	スイッチのホスト MAC アドレスを表示します。
VLAN	スイッチに構成された VLAN を表示します。
ポート	
L2 VNI	スイッチに構成されているレイヤ 2 VXLAN ネットワーク識別子（L2 VNI）を表示します。
L3 VNI	スイッチに設定されているレイヤ 3 VXLAN ネットワーク識別子（L3 VNI）を表示します。

容量（Capacity）

スイッチの物理容量を表示できます。

[キャパシティ（Capacity）] タブには、スイッチに存在する物理ポートに関する情報が表示されます。

[キャパシティ（Capacity）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列でスイッチ名をクリックして、**[キャパシティ（Capacity）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *2:* 容量タブ

フィールド	説明
階層	スイッチで使用可能な物理ポートを表示します。
使用済みポート	スイッチの使用ポート数を表示します。
合計ポート数	スイッチのポート数を表示します。
残り日数	残りの合計日数を表示します。

機能

スイッチで有効になっている機能を表示できます。

[機能（Features）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列のスイッチ名をクリックし、**[機能（Features）]** タブに移動します。

VXLAN

VXLAN タブで、VXLAN とその詳細を表示できます。

VXLAN を表示するには、**[モニタ（Monitor)] > [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）]** 列でスイッチ名をクリックします。

次の表に、表示されたフィールドの説明を示します。

表 *3: VXLAN* タブ

フィールド	説明
VNI	スイッチに設定されているレイヤ 2 (ネットワーク) またはレイヤ 3 (VRF) VXLAN VNI を表示します。
マルチキャスト アドレス。	該当する場合、レイヤ 2 VNI に関連付けられているマルチキャストアドレスを表示します。
VNI ステータス	VNI のステータスを表示します。
モード	VNIモードを表示します。コントロールプレーンまたはデータ プレーン。
タイプ	VXLAN VNI がネットワーク (レイヤー 2) または VRF (レイヤー 3) に関連付けられているかどうかを表示します。

フィールド	説明
VRF	レイヤ 3 VNI の場合、VXLAN VNI に関連付けられている VRF 名を表示します。
マッピングされた VLAN	VNI にマッピングされている VLAN またはブリッジ ドメインを表示します。

VLAN

[VLAN] タブで、VLAN とその詳細を表示できます。

VLAN を表示するには、**[モニタ（Monitor)] > [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）]** 列でスイッチ名をクリックします。

次のテーブルでは、表示されるフィールドについて説明します。

表 4 : [VLAN] タブ

フィールド	説明
VLAN	スイッチに構成した VLAN を表示します。
Name	VLAN の名前を表示します。
タイプ	ネットワークに関連付けられている VLAN が表示されます。
ポリシー	関連付けられたポリシーの名前を表示します。ポリシーが関連付けられていない場合、デフォルトでは未定義です。
モード	VLAN モードを表示します。
Status	VLAN のステータスを表示します。
ポート	VLAN がスイッチに物理的に接続されているポート番号を指定します。

スイッチ モジュール

[モジュール（Modules）] タブで、スイッチ モジュールとその詳細を表示できます。

To view the **[モジュール（Modules）]** タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列のスイッチ名をクリックし、**[モジュール（Modules）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *5:* モジュール タブ

フィールド	説明
名前	モジュールの名前を指定します。
ModelName	モジュールのモデル名を指定します。
SerialNum	モジュールのシリアル番号を指定します。
タイプ	モジュール タイプを指定します。有効な値は、**[シャーシ（chassis）]**、**[モジュール（module）]**、**[ファン（fan）]**、および **powerSupply** です。
OperStatus	モジュールの操作ステータスを指定します。
スロット	モジュールのスロット番号を指定します。
H/W 改定	NX-OS ハードウェア バージョンを指定します。
S/W 改訂	NX-OS ソフトウェア バージョンを指定します。
AssetID	モジュールのアセット ID を指定します。
IO FPGA	IO フィールド プログラマブル ゲート アレイ (FPGA) バージョンを指定します。
MI FPGA	MI フィールド プログラマブル ゲート アレイ（FPGA）のバージョンを指定します。

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。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 Fabric Extender（FEX; ファブリックエクステンダ）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 *6 : FEX*動作

フィールド	説明
表示する	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）] エリアに表示されます。変数を確認し、**[実行（Execute）]** をクリックします。出力は **[出力（Output）]** エリアに表示されます。 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。

表 *7 : 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。

フィールド	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。
州	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。
通番	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。

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 *8 : 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（Edit）] をクリックして VDC 構成を編集します。
削除	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（Delete）] 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。
一時停止	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 の実行構成をスタートアップ構成に保存します。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。
表示する	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（Interface）] 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（Resource）] 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 *9 : 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
Status	VDC のステータスを指定します。

フィールド	説明
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 • 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（General Parameter）] タブで、VDC **名**、**単一スーパーバイザ HA ポリシー**、**デュアル スーパーバイザ HA ポリシー**、および**リソース制限 - モジュール タイプ**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（Allocate Resource）] タブで、VDC のリソース制限を指定します。

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 リソースの制限については、以下で詳しく説明します。

表 *10:* テンプレート リソースの制限

Resource	最小	最大
グローバル デフォルト VDC テンプレート リソースの制限		
エニーキャスト同梱		
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。

Resource	最小	最大
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		
SRC INBAND のモニタ		
ポート チャネル		
DST ERSPAN のモニタ		
SPAN セッション		
VLAN		
エニーキャスト同梱		
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		

- **[新しいリソース 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。[リソース制限（Resource Limits）] 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 Client] > [Inventory] > [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（Authenticate）] 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。

[管理ユーザー（Admin User）] 領域で：

- 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 [概要（Summary）] 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（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（Deploy）] 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** 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]** 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（Authenticate）] 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。

[管理ユーザー（Admin User）] 領域で：

- 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 [概要（Summary）] 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（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（Deploy）] 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（Switch）]** 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。

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 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 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

LAN 収集画面から 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（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]

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。

LAN スイッチの温度モニタリングの有効化

1. **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [ローカル エリア ネットワーク（LAN） コレクション（LAN Collections）]** をメニュー バーから選択します。
2. **[温度センサー（Temperature Sensor）]** チェック ボックスを選択します。
3. 性能データを収集したい LAN スイッチの種類を選択します。
4. [Apply] をクリックして、設定を保存します

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（Monitor）] > [スイッチ（Switch）] > [アカウンティング（Accounting）]**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、**[抑制の追加（Add Suppressor）]** アイコンをクリックして、イベント抑制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。

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、および昨年で表示するようにフィルタできます。

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 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有効化します。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、2 分割帯域幅を増やす拡張された形式のポートチャネルです。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（Deploy）] > [vPC ピア（vPC Peer）]** および **[Web クライアント（Web Client）] > [構成（Configure）] > [展開（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 11: vPC パフォーマンス, on page 31 は、データ グリッド 表示に次の vPC 構成の詳細を表示します。

***Table 11: 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処理します。
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 識別子 を表示します。
[マルチ シャーシ vPC エンドポイント（Multi Chassis vPC EndPoints）]	vPC ドメインの下の各 vPC 識別子 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（Primary vPC Peer - Device Name）]	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（Primary vPC Peer - Primary vPC Interface）]	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 - キャパシティ（Primary vPC Peer - Capacity）]	プライマリ vPC ピアのキャパシティを表示します。
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。

列	説明
[プライマリ vPC ピア - ピーク使用率（Primary vPC Peer - Peak Util%）]	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（econdary vPC Peer - Device Name）]	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（Secondary vPC Interface）]	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 - キャパシティ（Secondary vPC Peer - Capacity）]	セカンダリ vPC ピアのキャパシティを表示します。
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（Secondary vPC Peer - Peak Util%）]	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（vPC Details）]**、**[ピア リンクの詳細（Peer-link Details）]**、および **[ピア リンクのステータス（Peer-link Status）]** が表示されます。

vPC の **[vPC 整合性（vPC Consistency）]**、**[ピア リンク整合性（Peer-link Consistency）]**、および **[vPC Type2 整合性（vPC Type2 Consistency）]** が表示されます。

- **[vPC の詳細（vPC Details）]** 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（Basic Setting）]** と **[レイヤ 2 設定（Layer 2 Settings）]** のパラメータの詳細を表示できます。
- **[ピア リンクの詳細（Peer-link Details）]** 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（vPC Global Setting）]** および **[STP グローバル設定（STP Global Settings）]** 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（Peer-link Status）]** タブをクリックすると、**[vPC の整合性（vPC Consistency）]** が表示され、**[ピア リンクの整合性（Peer-Link Consistency）]** 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（Role Status）]** と **[vPC ピア キープアライブ ステータス（vPC Peer keep-alive Status）]** 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（Primary vPC peer）]** または **[セカンダリ vPC ピア（Secondary vPC peer）]** 列の **[デバイス名（Device Name）]** 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。

- 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。

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このランディング ページに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によって異なります。

- エンドポイント ロケータ
- エンドポイント ロケータの監視

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）、シビラティ（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、コンピューティング 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、各コンピューティング ノードで **appmgr backup** コマンドを実行します。

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（Device Health）]**：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（Interface Health）]**：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 Alarm）]**：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（Enable Alarms）]** 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 12:* 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 13:* 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 14:* 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（Activate）]** 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（Deactivate）]** 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。

構成コンプライアンス アラーム

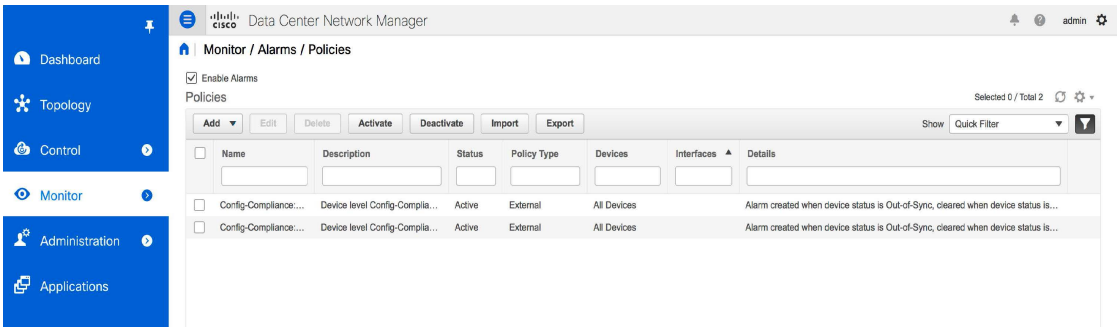
Cisco DCNM リリース 11.3(1) 以降、外部カテゴリの下のアラーム ポリシーとアラームは、DCNM で実行されているアプリケーションによって作成されます。これらの外部アラーム ポリシーはアプリケーションによって作成され、DCNM Web UI を介して作成または追加することはできません。

Config-Compliance(CC) は、DCNM で実行されるコア アプリケーションです。CC は、外部アラーム カテゴリの下にアラームを登録および作成します。

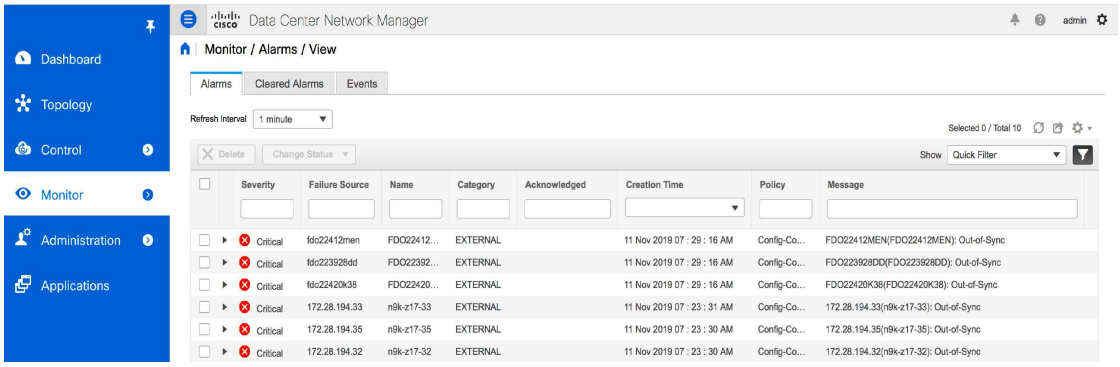
Config-Compliance : アラーム ポリシー

この外部アラーム カテゴリ ポリシーは、ファブリックの作成時にアクティブ化され、そのファブリック内のすべてのデバイスで有効になります。ポリシーの重大度レベルは重大です。ファブリック内のいずれかのデバイスが In-Sync から Out-of-Sync に移動し、**[アラームを有効化（Enable Alarms）]** チェックボックスが選択されている場合、重大な重大度のアラームが生成されます。

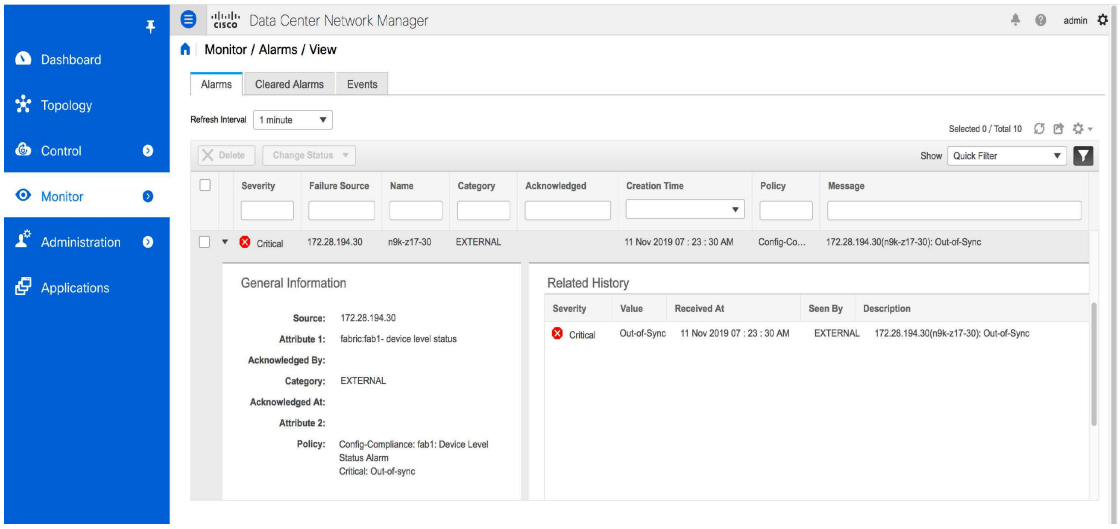
[モニタ（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）] を選択して、デフォルトのアラーム ポリシーを表示します。このアラームポリシーは、Web UI では編集できません。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、選択したポリシーをアクティブ化または非アクティブ化します。



DCNM Web UI 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、DCNM Web UI からはポリシーを削除しないことをお勧めします。ポリシーが削除された場合、CC は、次回の定期実行時、またはデバイス レベルまたはそのファブリックの下のファブリック レベルで再同期がトリガーされたときに、ポリシーを再生成します。



アラームの詳細な情報を表示するには**[重大（Critical）]**の横にある矢印アイコンをクリックします。

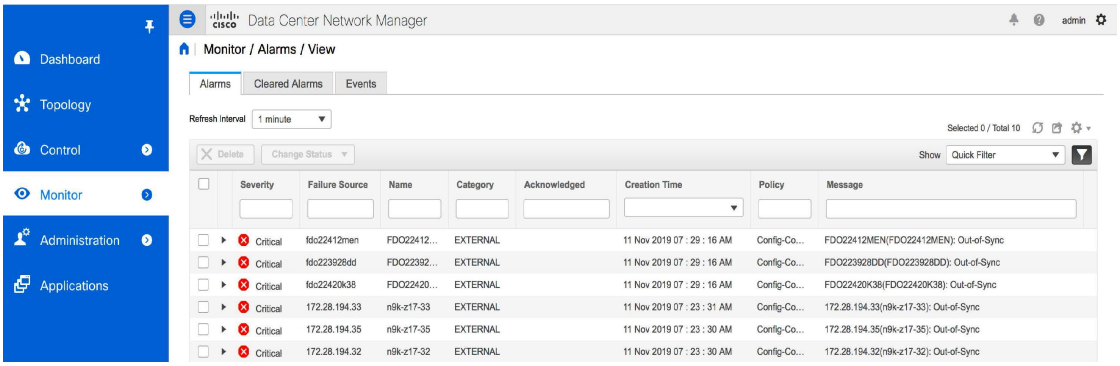


Out-of-Sync ステータスは、DCNM でデバイスに定義されたインテントとデバイスで実行中の構成との間に違いがあることを示します。In-Sync ステータスは、DCNM でデバイスに定義されたインテントが実行構成と一致し、CC が構成間に違いを検出しなかったことを示します。差分の計算の詳細については、「*DCNM* での構成の準拠」を参照してください。

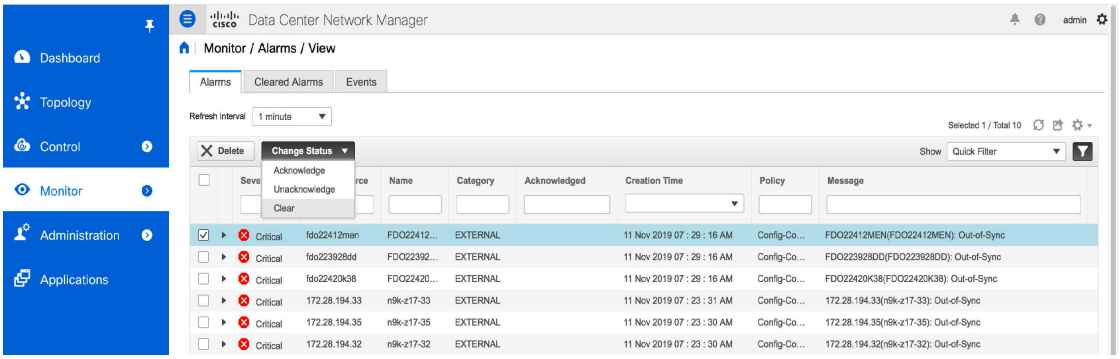
ファブリックが削除されると、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

Config-Compliance：アクティブ アラーム

CC がファブリックで実行されていて、そのファブリック内のデバイスが Out-of-Sync ステータスに移行するシナリオを検討してください。これにより、重大な重大度アラームが生成されます。**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** を選択して、アラームを表示します。これらのアラームは、デバイスが Out-of-Sync から In-Sync に移行するまでアクティブです。



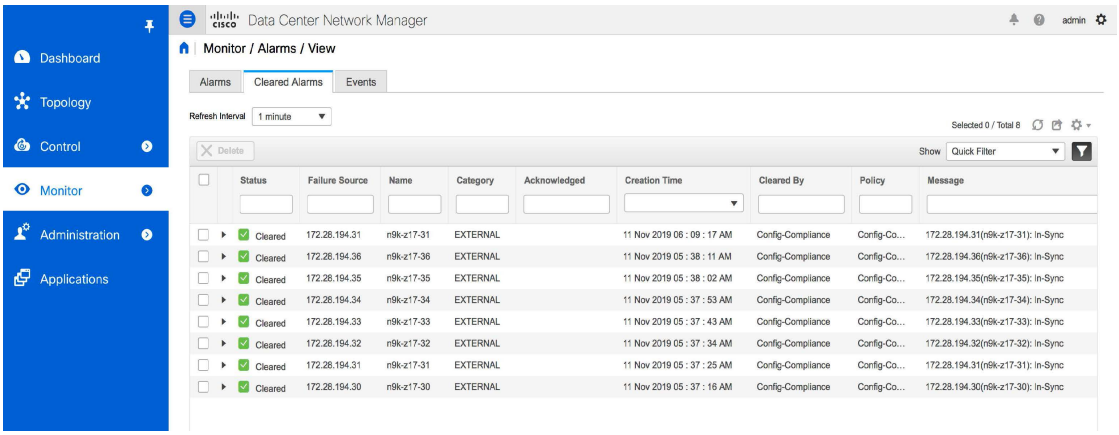
アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[ステータスを変更（Change Status）]**をクリックして**[クリア（Clear）]** を選択します。同じデバイスが再び Out-of-Sync ステータスに移行すると、アクティブなアラームが再作成されます。



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。同じデバイスが再び Out-of-Sync ステータスに移行すると、アクティブなアラームが再作成されます。

Config-Compliance：クリアされたアラーム

Out-of-Sync ステータスにあるデバイスが In-Sync ステータスに移行すると、現用系アラームがクリアされます。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。クリアされたアラームは、全体的なデバイス 正常性スコアには影響しません



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、**[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、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。これにより、選択したクリア済みアラームがリストから削除されます。

スイッチが Out-of-Sync から In-Sync に移動すると、アラームはクリアされます。構成コンプライアンス アラームは、デバイスの全体的な正常性スコアにも影響します。

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。

エンドポイント ロケータ アラーム

Cisco DCNM リリース 11.4(1) よりアラームは、エンドポイントロケータ（EPL）によって外部アラーム カテゴリに登録および作成されます。

エンドポイント ロケータ：アラーム ポリシー

EPL 外部アラームカテゴリポリシーは、ファブリックで EPL が有効になっているときにアクティブになります。アラームは、重複する IP アドレス、重複する MAC アドレス、VRF に表示されるエンドポイント、VRF から消えるエンドポイント、ファブリック内で移動するエンドポイント、ルートリフレクタ接続の喪失、ルートリフレクタ接続の復元などの問題に対して発生します。問題に応じて、アラームポリシーの重大度レベルは CRITICAL または MINOR になります。

アラームは、次のイベントに対して発生し、CRITICAL に分類されます。

- ルートリフレクタの切断
- 重複する IP アドレスの検出
- 重複する MAC アドレスの検出

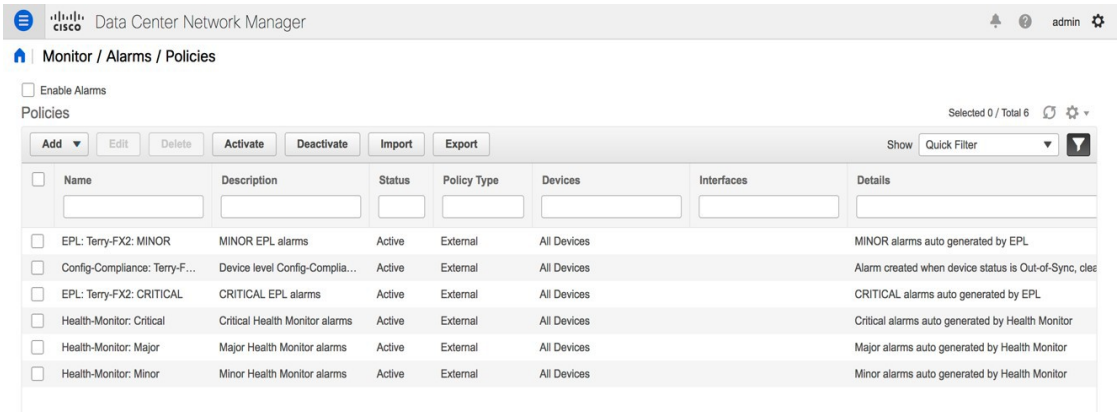
次のイベントの場合、アラームが発生し、MINOR として分類されます。

- エンドポイントの移動
- ファブリック内の新しい VRF の表示

- ファブリック内のエンドポイントの数が 0 になる
- VRF のエンドポイントの数が 0 になる
- スイッチからのすべてのエンドポイントの消失
- ルートリフレクタ（RR）の接続

状態が修正されると、CRITICAL アラームは自動的にクリアされます。たとえば、DCNM と RR 間の接続が失われると、CRITICAL アラームが生成されます。このアラームは、DCNM と RR 間の接続が回復すると自動的にクリアされます。その他の MINOR アラームは、アラームが生成されてから 30 分が経過すると自動的にクリアされます。

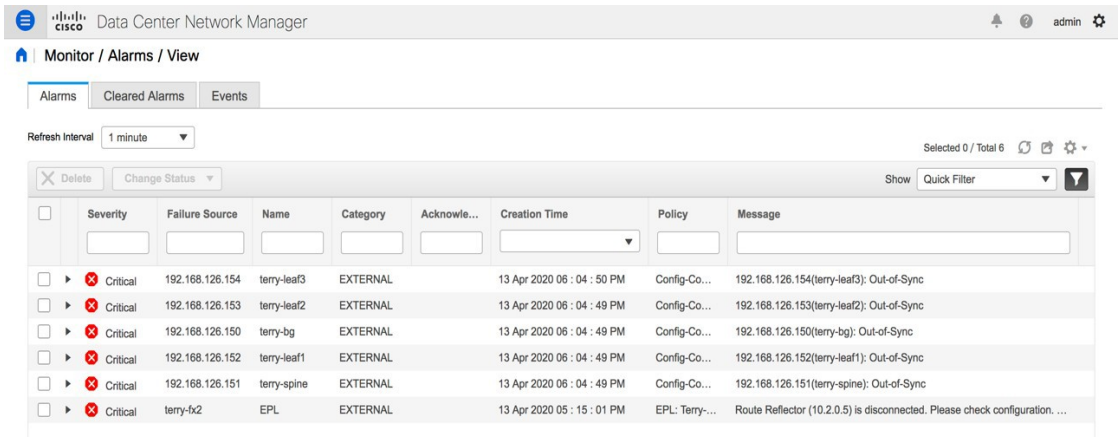
[モニタ（Monitor）] > [アラーム（Alarm）] > [ポリシー（Policies）] を選択して、EPL アラームポリシーを表示します。これらのアラームポリシーは、Web UI では編集できません。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、選択したポリシーをアクティブ化または非アクティブ化します。



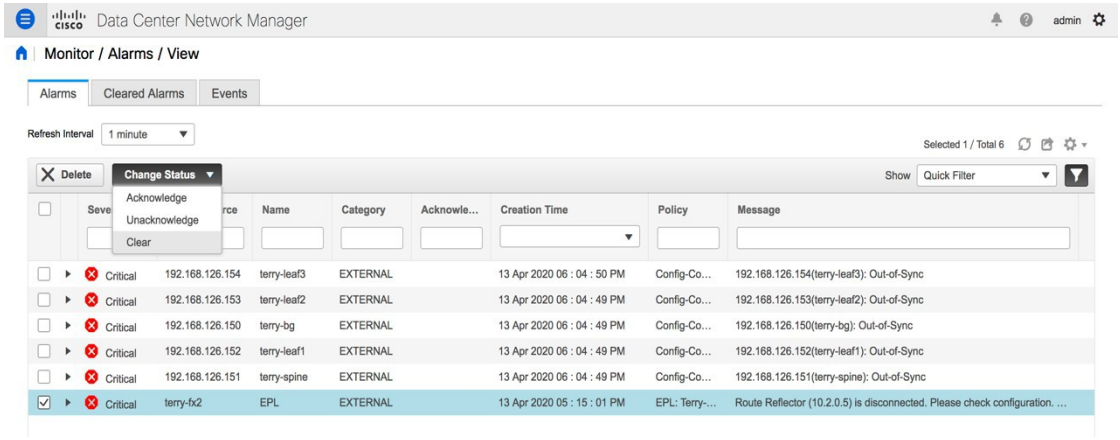
DCNM Web UI を使用してアラーム ポリシーが非アクティブ化された場合、そのポリシーに対して作成またはクリアされたアラームは、**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。ただし、DCNM Web UI からはポリシーを削除しないことをお勧めします。ファブリックが削除されると、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

エンドポイントロケータ：アクティブアラーム

[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。



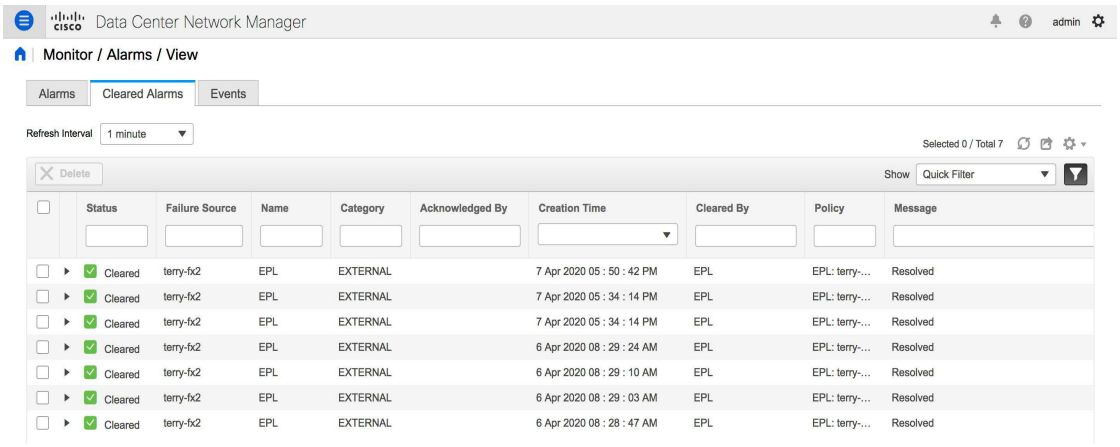
アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[ステータスを変更（Change Status）]**をクリックして **[クリア（Clear）]** を選択します。



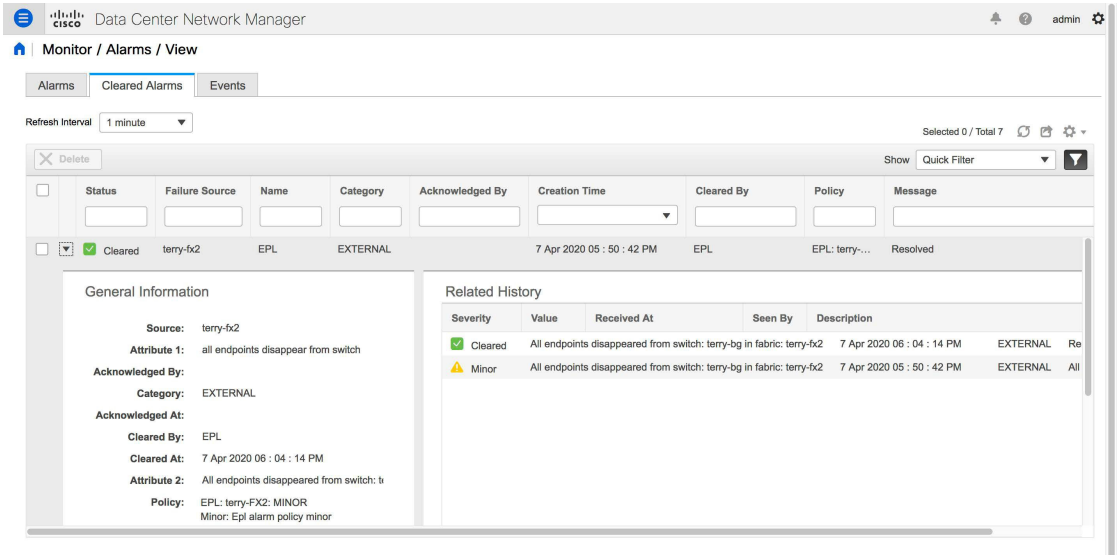
アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。

エンドポイントロケータ：クリアされたアラーム

クリアされたアラームを表示するには **[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。

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%

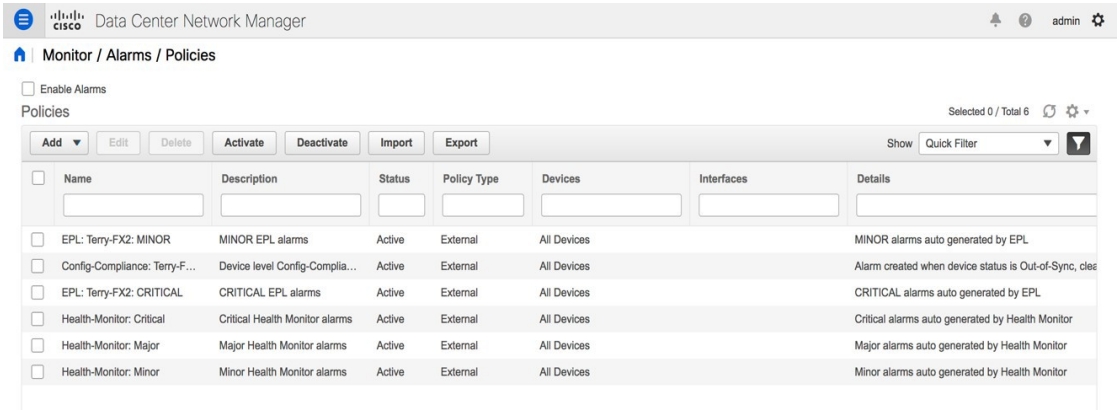
次のイベントの場合、アラームが発生し、メジャーとして分類されます。

- 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。