インベントリ

この章は次のトピックで構成されています。

インベントリ情報の表示

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

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

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

[Inventory] メニューには、次のサブメニューがあります。

スイッチのインベントリ情報の表示

Cisco DCNM Web UI のスイッチのインベントリ情報を表示するには、次の手順を実行します。

Procedure

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

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

ステップ 2 次の情報が表示されます。

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

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

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

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

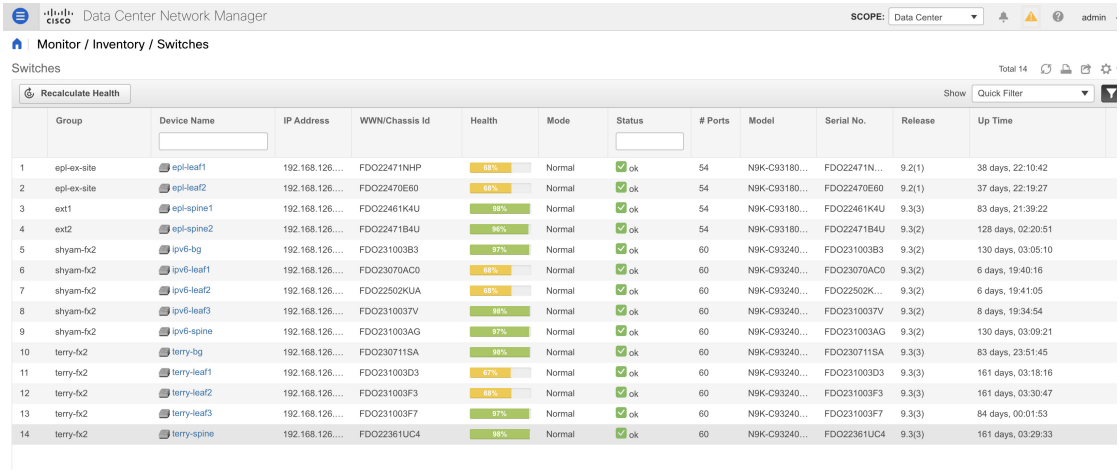
  コンテナ ベースの ISSU は、Cisco Nexus 3164Q、9200 シリーズ スイッチ、9332PQ、9372PX、9372TX、9396PX、9396TX、93120TX、および 93128TX スイッチでサポートされています。

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

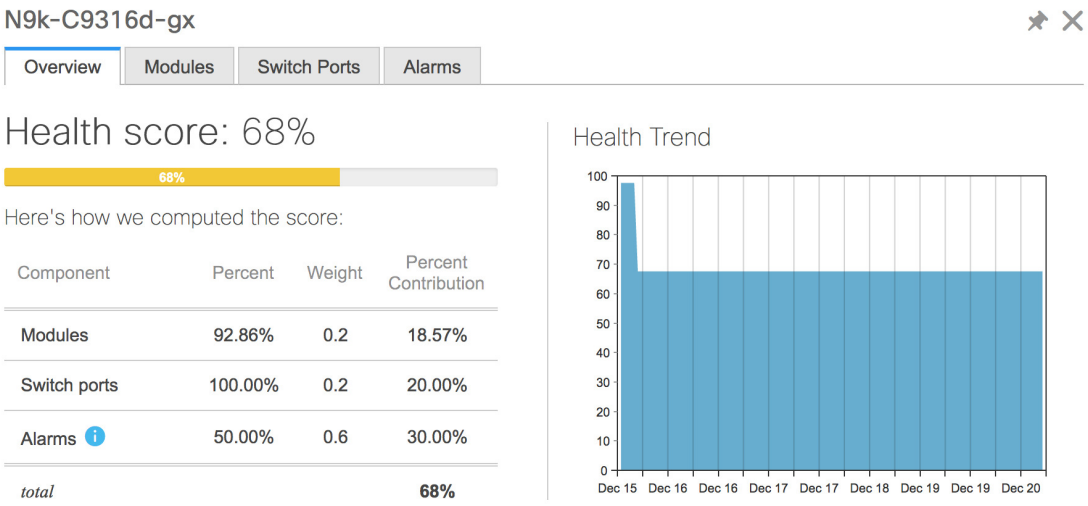
Cisco Nexus 9000 シリーズ NX-OS リリース 9.x ソフトウェア アップグレード/ダウングレード ガイド

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

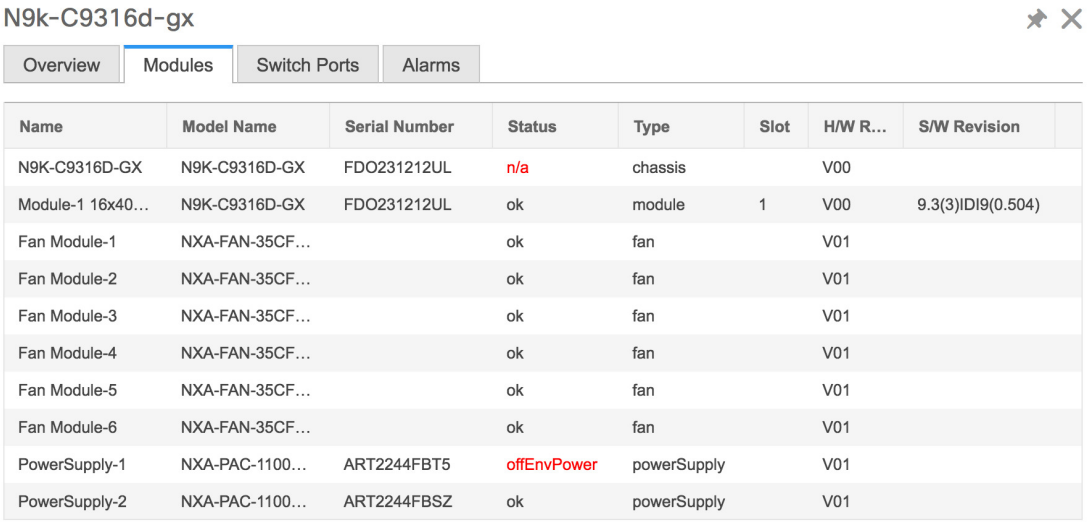
Cisco NX-OS ISSU サポート マトリクス



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

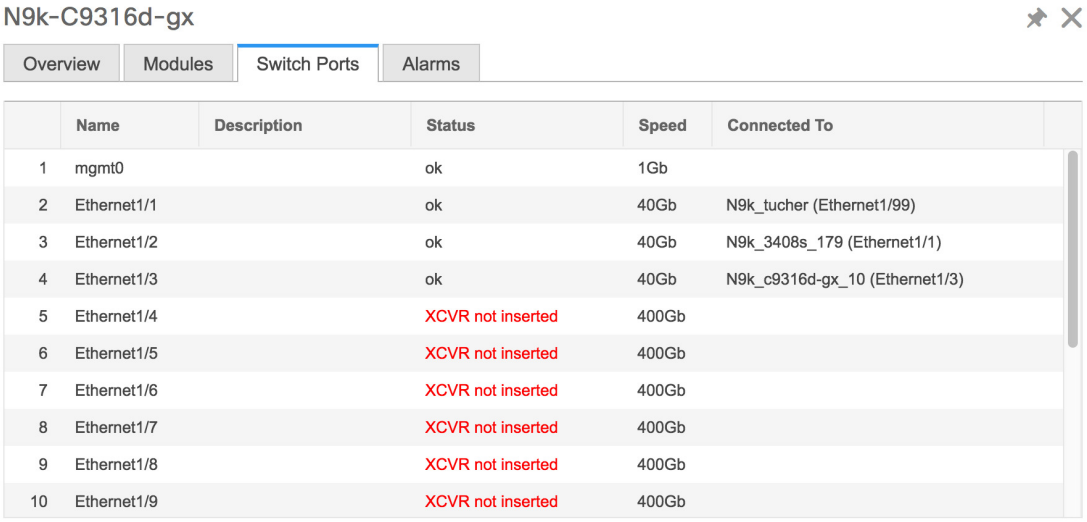


[モジュール（Modules）] タブをクリックして、デバイスのさまざまなモジュールに関する情報を表示します。このタブには、名前、モデル名、シリアル番号、ステータス、タイプ、スロット、ハードウェア リビジョン、ソフトウェア リビジョンなどの情報が表示されます。



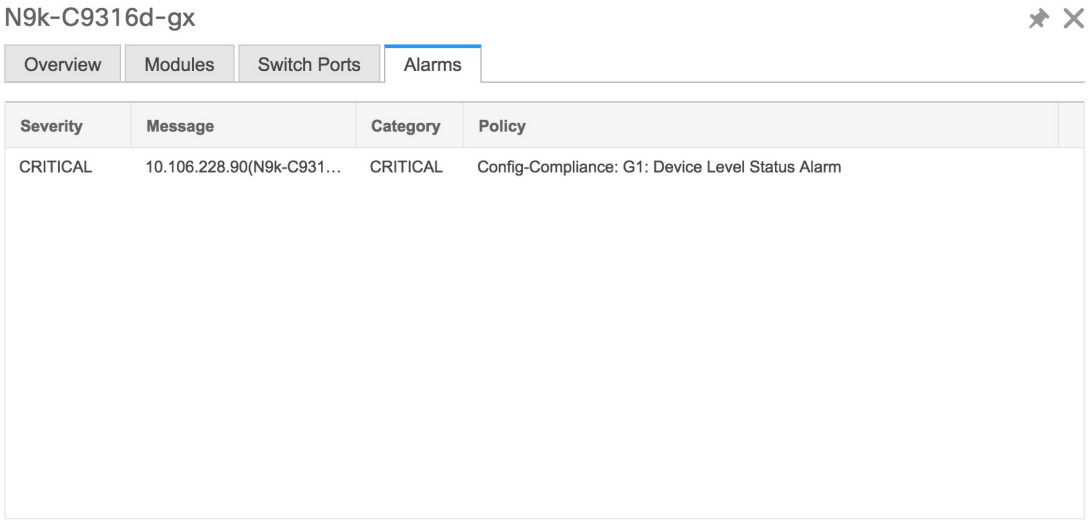
Name	Model Name	Serial Number	Status	Type	Slot	H/W R...	S/W Revision
N9K-C9316D-GX	N9K-C9316D-GX	FDO231212UL	n/a	chassis		V00	
Module-1 16x40...	N9K-C9316D-GX	FDO231212UL	ok	module	1	V00	9.3(3)IDI9(0.504)
Fan Module-1	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-2	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-3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

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



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

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



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

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

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

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

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

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

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

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

システム情報の表示

スイッチのダッシュボードには、選択したスイッチの詳細が表示されます。

Procedure

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

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

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

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

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

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

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

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

デバイスからテクニカル サポートの収集

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

Procedure

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

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

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

そのスイッチに対応するスイッチのダッシュボードが表示されます。

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

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

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

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

Note このオプションは、Nexus スイッチでのみ有効です。

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

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

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

ステップ 6 [OK] をクリックします。

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

デバイス マネージャ情報の表示

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

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

スイッチのダッシュボードには、選択したスイッチの詳細が表示されます。

Procedure

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

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

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

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

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

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

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

スイッチ ライセンスのインストール

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

Procedure

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

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

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

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

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

ステップ 4 **[ライセンス ファイルの選択（Select License File）]** をクリックし、ローカル システムからライセンス ファイルを選択します。

ステップ 5 送信メソッドの選択。次のオプションを使用できます。

- TFTP
- SCP
- SFTP

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

ステップ 7 [インストール（Install）] をクリックします。

スイッチ ライセンスの再検出

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

手順

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

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

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

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

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

スイッチ ライセンスの再検出には時間がかかります。

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

インターフェイス

インターフェイスの show コマンドの表示

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

手順

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

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

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

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

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

インターフェイスの再検出

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

手順

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

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

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

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

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

インターフェイス履歴の表示

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

手順

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

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

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

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

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

VLAN

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

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

次の表で、このページに表示されるボタンを説明します。

表 1 : VLAN タブ

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

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

この項の内容は、次のとおりです。

VLAN の追加

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

手順

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

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

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

ステップ 3 **[VLAN]** タブをクリックします。

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

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

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

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

VLAN の有効化

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

手順

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

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

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

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

VLAN の削除

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

手順

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

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

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

ステップ 3 **[VLAN]** タブをクリックします。

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

VLAN のシャットダウン

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

手順

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

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

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

ステップ 3 **[VLAN]** タブをクリックします。

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

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

VLAN Show コマンドの表示

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

手順

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

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

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

ステップ 3 **[VLAN]** タブをクリックします。

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

FEX

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

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

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

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

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

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

（注） FEX タブは、LAN デバイスを選択した場合にのみ表示されます。

次の表で、このページに表示されるフィールドを説明します。

表 *2 : FEX*動作

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

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

表 *3: FEX* フィールドと説明

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

この章は、次の項で構成されています。

FEX を追加

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

始める前に

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

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

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

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

手順

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

[FEX] ウィンドウが表示されます。

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

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

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

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

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

識別子は、100 から 199 までの整数値である必要があります。

ステップ 6 [追加] をクリックします。

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

FEX の編集

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

手順

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

[FEX] ウィンドウが表示されます。

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

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

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

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

ステップ 5 [プレビュー（Preview）] をクリックします。

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

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

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

VDC

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

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

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

次の表で、このページに表示されるフィールドを説明します。

表 *4: VDC* オペレーション

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

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

表 *5 : VRF* テーブルのフィールドと説明

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

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

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

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

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

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

この章は、次の項で構成されています。

VDC の追加

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

始める前に

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

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

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

手順

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

VDC ウィンドウが表示されます。

ステップ 2 **[追加（Add）]** アイコンをクリックします。

ステップ 3 ドロップダウン リストから、VDC タイプを選択します。

VDC は 2 つのモードで構成できます。

- イーサネット VDC の構成

- ストレージ VDC の構成

デフォルトの VDC タイプは Ethernet です。

ステップ 4 [OK] をクリックします。

イーサネット *VDC* の構成

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

手順

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

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

[次へ（Next）] をクリックします。

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

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

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

  テンプレート 技術情報の制限については、以下で詳しく説明します。

表 *6:* テンプレート 技術情報の制限

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

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

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

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

[次へ（Next）] をクリックします。

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

管理者ユーザーエリアで：

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

AAA サーバ グループ エリア内：

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

[次へ（Next）] をクリックします。

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

[次へ（Next）] をクリックします。

ステップ 6 サマリ タブ内で VDC 構成を確認します。

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

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

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

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

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

ストレージ *VDC* の構成

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

始める前に

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

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

手順

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

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

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

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

[次へ（Next）] をクリックします。

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

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

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

[次へ（Next）] をクリックします。

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

管理者ユーザーエリアで：

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

AAA サーバ グループ エリア内：

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

[次へ（Next）] をクリックします。

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

[次へ（Next）] をクリックします。

ステップ 6 サマリ タブ内で VDC 構成を確認します。

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

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

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

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

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

VDC の編集

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

手順

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

VDC ウィンドウが表示されます。

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

ステップ 3 必要に応じてパラメータを変更します。

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

モジュールのインベントリ情報の表示

Cisco DCNM Web UI の モジュール のインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ（Inventory）] > [表示（View）] > [モジュール（Modules）]**の順に選択します。

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

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、モジュールのグループ名が表示されます。
- **[スイッチ（Switch）]** 列には、モジュールが検出される時にスイッチ名が表示されます。
- **[名前（Name）]** にはモジュール名が表示されます。
- **[ModelName]** にモデル名が表示されます。
- **[SerialNum]** 列には、シリアル番号が表示されます。
- **[2nd SerialNum（2 番目の SerialNum ）]** 列には、 2 番目シリアル番号が表示されます。
- **[タイプ（Type）]** 列には、モジュールのタイプが表示されます。
- **[スロット（Slot）]** 列には、スロット番号が表示されます。
- **[ハードウェア リビジョン（Hardware Revision）]**列には、モジュールのハードウェア バージョンが表示されます。
- **[ソフトウェア リビジョン（Software Revision）]** 列には、モジュールのソフトウェア バージョンが表示されます。

- **[アセット ID（Asset ID）]** カラムには、モジュールのアセット ID が表示されます。
- **[OperStatus]** 列には、デバイスの動作状態が表示されます。
- **[IO FPGA]** 列には、IO フィールド プログラマブル ゲート 配列（FPGA）バージョンが表示されます。
- **[MI FPGA]** 列には、MI フィールド プログラマブル ゲート 配列（FPGA）のバージョンが表示されます。

ライセンスのインベントリ情報の表示

Cisco DCNM Web UI のライセンスのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[インベントリ] > [表示] > [ライセンス]** の順に選択します。

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

ステップ 2 次の情報が表示されます。

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

ディスカバリ

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

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

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

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

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

この項の内容は、次のとおりです。

LAN スイッチの追加

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

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

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note .

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

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

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

ローカル エリア ネットワーク（LAN）デバイスの編集

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

Procedure

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

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

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

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

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

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

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

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

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

Procedure

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

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

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

タスクの下での LAN デバイスの移動

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

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

Procedure

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

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

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

選択したタスク配下のすべての LAN デバイスが移動されます。

LAN タスクの再検出

Procedure

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

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

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

管理されているファブリックの追加、編集、再検出、消去と削除。

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

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

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

この項の内容は、次のとおりです。

ファブリックの追加

Before you begin

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

Procedure

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

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

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

[ファブリックの追加（Add Fabric）] ウィンドウが表示されます。

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

ステップ 4 (Optional) **SNMP** チェックボックスをオンにして、SNMPv3 または SSH を使用します。[SNMP] チェックボックスをオンにすると、**[コミュニティ（Community）]** フィールドが **[ユーザー名（User Name）]** および **[パスワード（Password）]** に変わります。

ステップ 5 このファブリックに対して**ユーザー名**と**パスワード**を入力します。

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

ステップ 7 (Optional) **[VSAN による検出の制限（Limit Discovery by VSAN）]** チェックボックスをオンにして、新しいファブリックを検出するために提供された VSAN に含まれる VSAN リストまたは除外される VSAN リストを指定します。

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

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

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

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

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

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

ファブリックを削除しています

Procedure

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

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

ステップ 3 **[削除（Delete）]** をクリックして、データソースからファブリックを削除し、そのファブリックのデータ収集を中止します。

ファブリックの編集

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

Procedure

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

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

[ファブリックの編集（Edit Fabric）] ダイアログボックスが表示されます。一度に編集できるファブリックは 1 つだけです。

ステップ 3 新しいファブリックの **[名前（Name）]** を入力します。

ステップ 4 (Optional) [SNMPV3] チェックボックスをオンにします。SNMPV3 をオンにすると、**[コミュニティ（Community）]** フィールドが **[ユーザー名（User Name）]** および **[パスワード（Password）]** に変わります。

ステップ 5 **[ユーザー名（Username）]** および **[パスワード（Password）]** 、[プライバシー（privacy）] を入力し、 いずれかのステータス オプションを選択することで、DCNM Web クライアントでファブリックを管理する方法を指定します。

ステップ 6 ファブリック管理状態を **[管理対象、非管理対象（Managed, Unmanaged）]** または **[継続的に管理（Managed Continuously）]** に変更します。

ステップ 7 [Apply] をクリックして、変更内容を保存します。

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

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

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

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

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

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

ファブリックを別のサーバ フェデレーションに移動する

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

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

Procedure

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

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

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

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

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

ファブリックの再検出

Procedure

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

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

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

ファブリックが再検出されました。

ファブリックの消去

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

Procedure

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

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

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

ファブリックは消去されます。

UCS ファブリック インターコネクト統合

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

ディスカバリを有効にする

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

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

UCS FI デバイスの検出

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

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

手順

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

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

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

[ファブリックの追加（Add Fabric）] ウィンドウが表示されます。

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

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

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

ステップ 5 ファブリックに対してユーザー名とパスワードを入力します。

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

ステップ 7 （任意） **[VSAN による検出の制限（Limit Discovery by VSAN）]** チェックボックスをオンにして、新しいファブリックを検出するために提供された VSAN に含まれる VSAN リストまたは除外される VSAN リストを指定します。

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

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

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

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

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

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

このオプションは、フェデレーションのセットアップだけに適用できます。

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

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

（注） UCS FI は、SNMP ユーザー管理の使用を禁止しています。

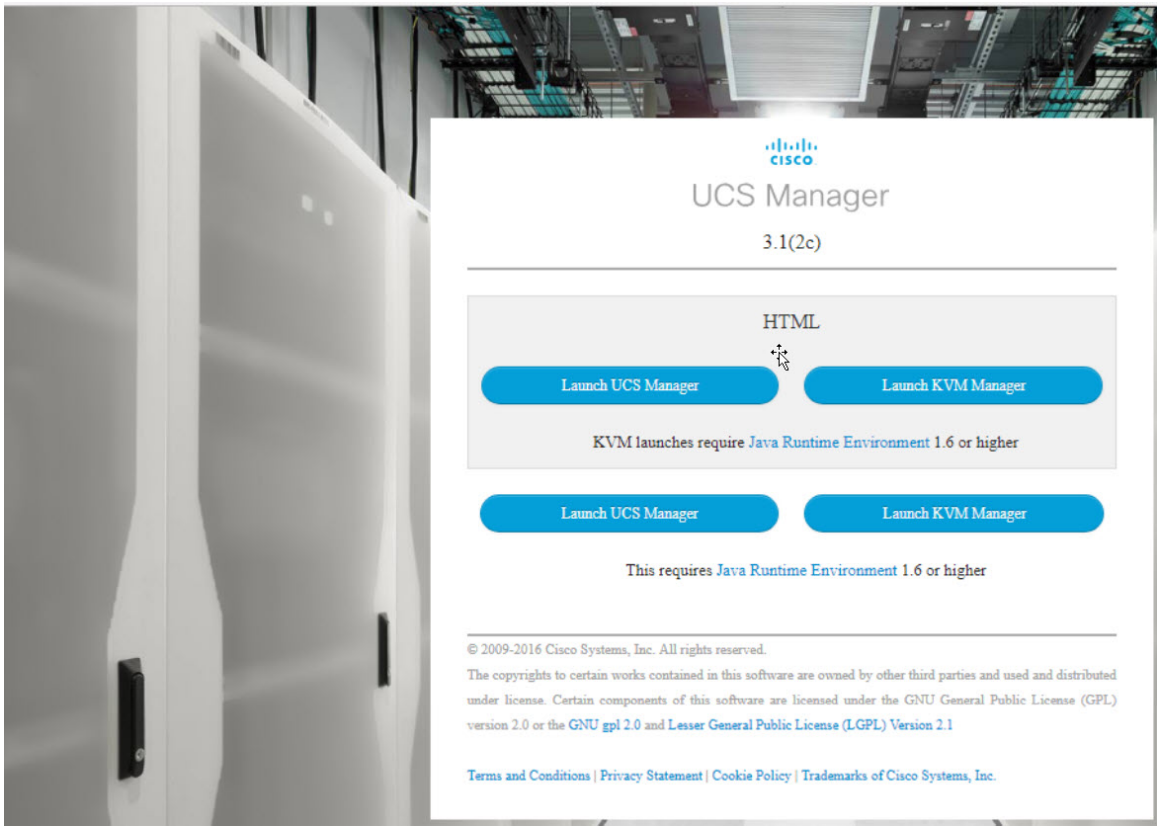
UCS FI での SNMP ユーザーの作成

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

手順

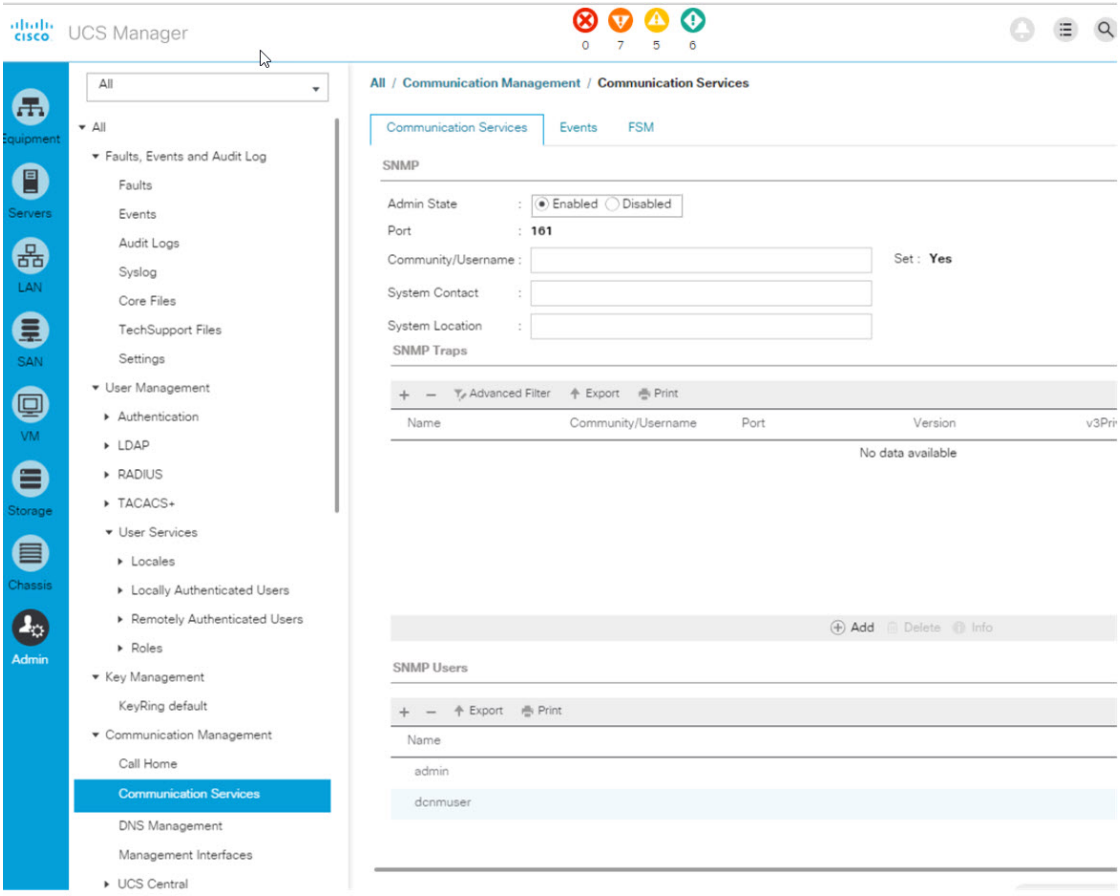
ステップ 1 UCS Manager にログインします。

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



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

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



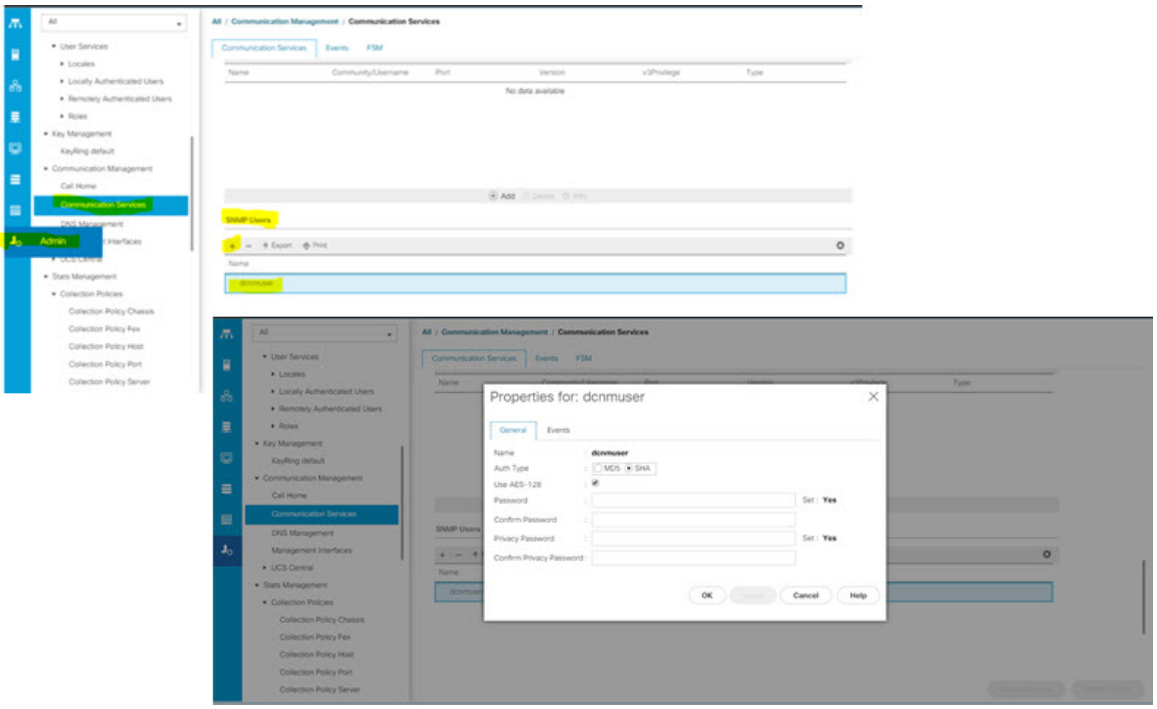
ステップ 4 新しい SNMP ユーザーを作成し、ログイン情報を提供します。

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

または、AES-128 暗号化で SHA を使用します。

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

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



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

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

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


User            Auth  Priv
____            ____  ____
```

これは、Cisco NPV スイッチにも当てはまります。

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

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

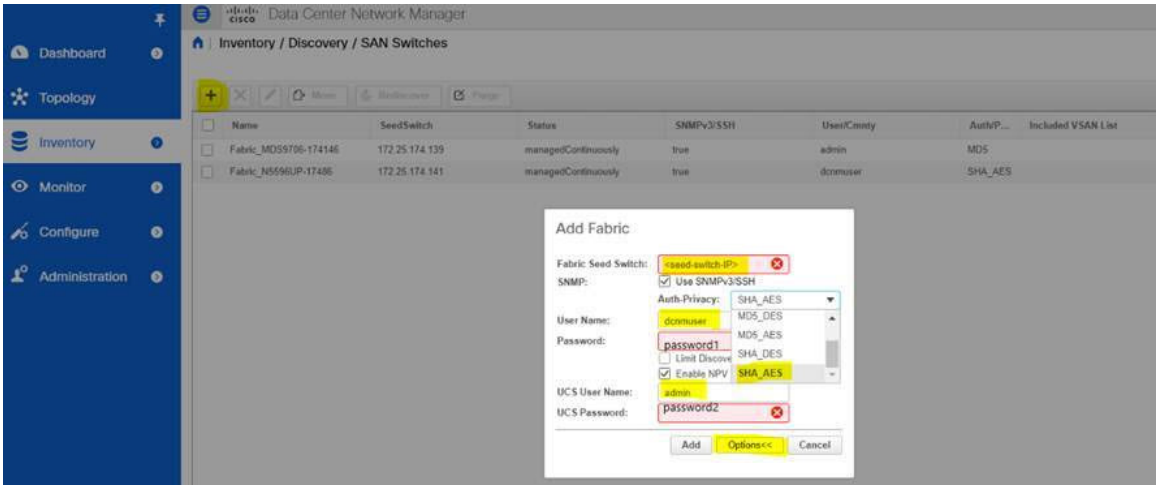
```
admin           md5   des(no)       network-admin
dcnmuser        sha   aes-128(no)   network-admin       network-operator
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________

User            Auth  Priv
____            ____  ____
```

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

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

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



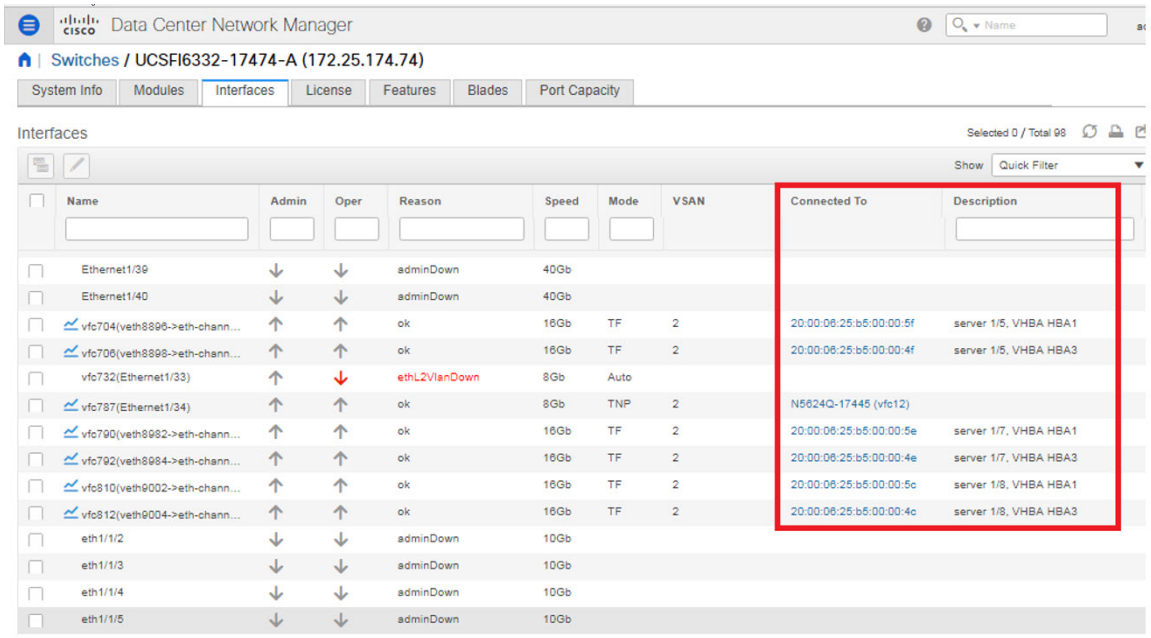
ステップ 7 UCF FI スイッチが Cisco DCNM **[Web UI] > [インベントリ（Inventory）] > [スイッチ（Switches）]** にリストされていることを確認します。

これらのスイッチのステータスが正しいことを確認してください。

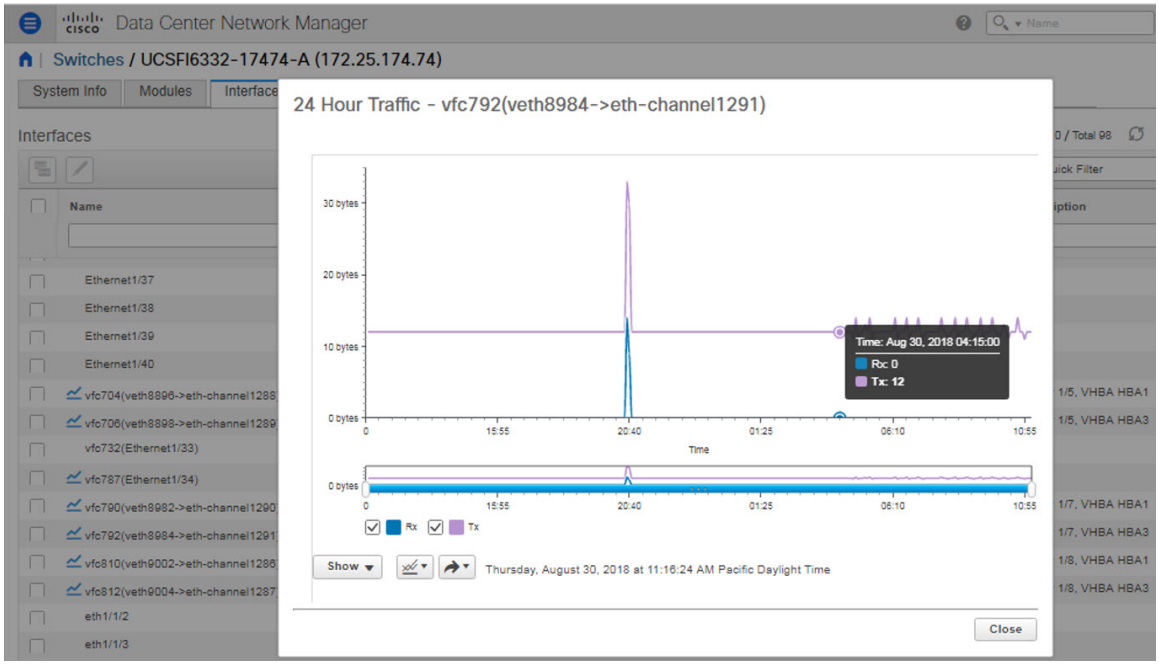
インベントリでの UCS FI スイッチの表示

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

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

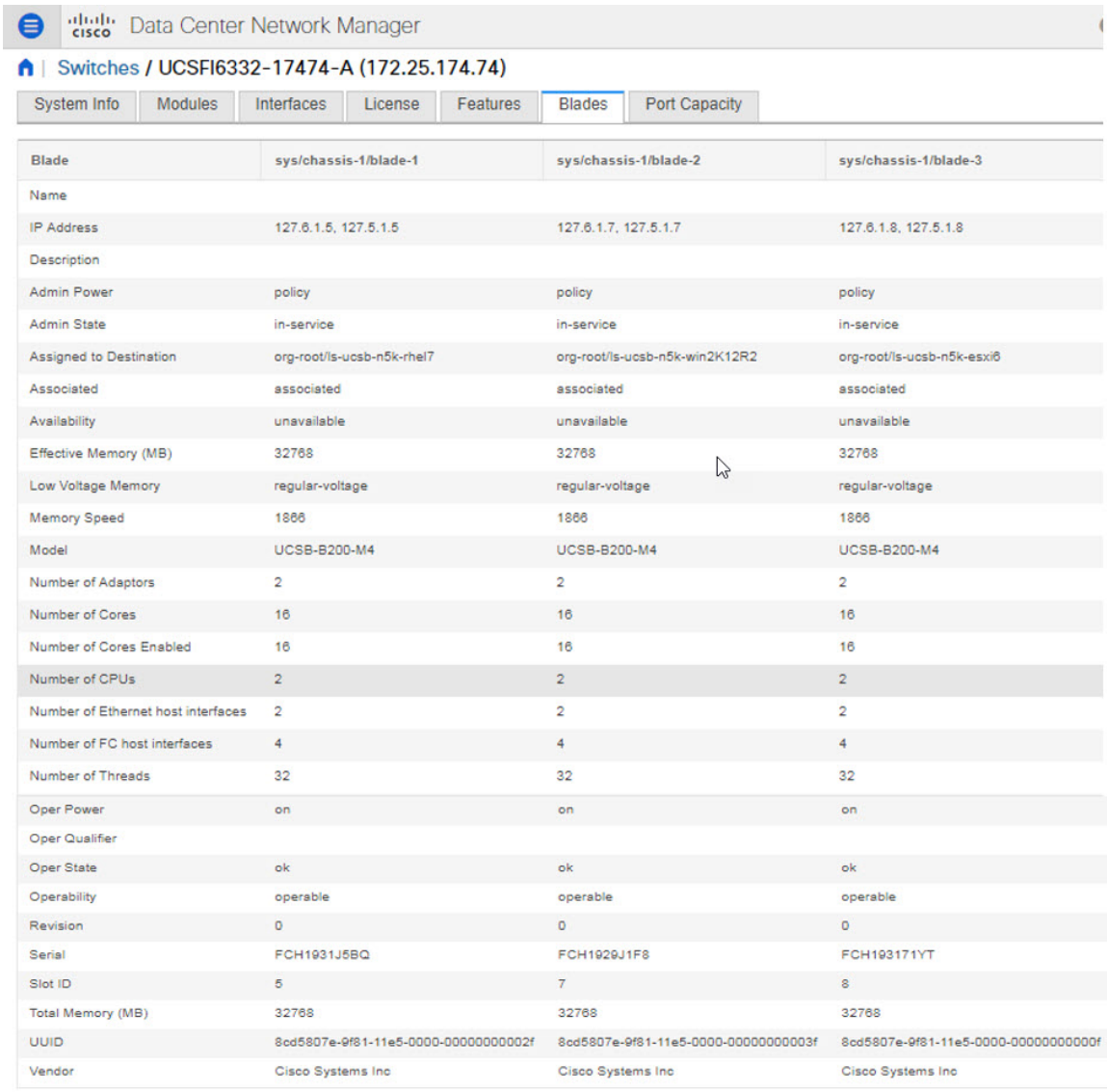


名前列の下のグラフ アイコンをクリックして、そのポートの 24 時間のトラフィック データを表示します。



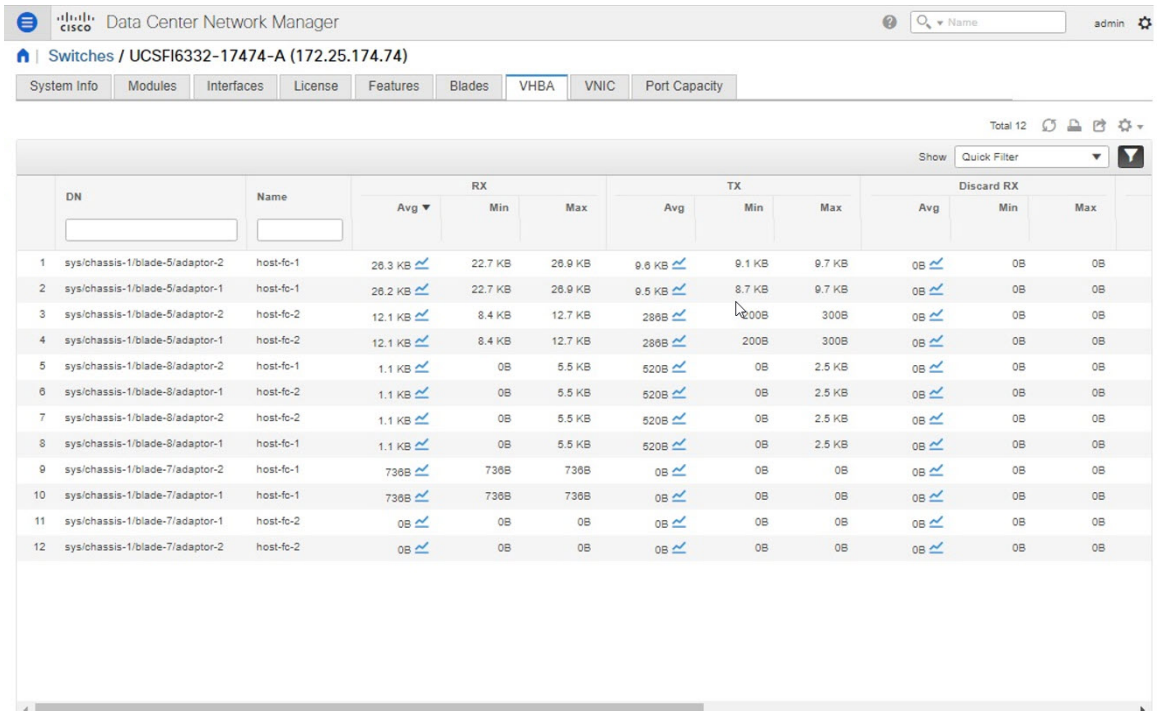
システム情報タブには、セカンダリ UCS FI に対応するプライマリ UCS FI IP が表示されます。

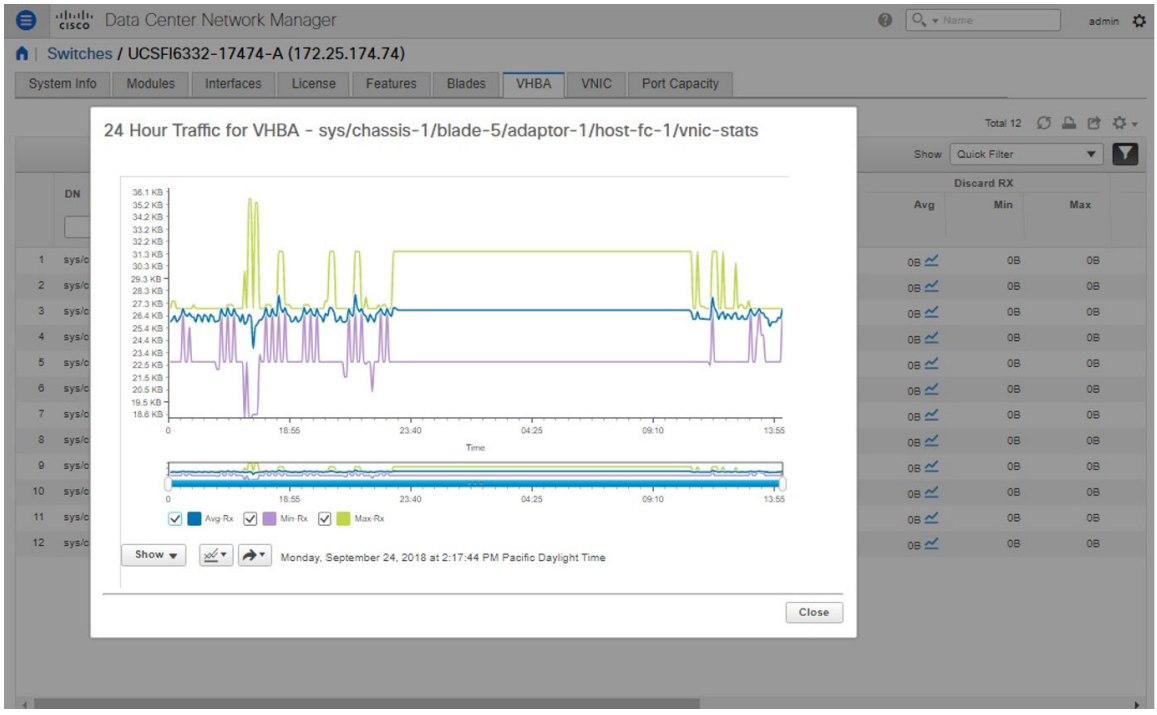
[ブレード（Blades）] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。冗長セットアップのプライマリ UCS FI またはスタンドアロン UCS FI のみが表示されます。



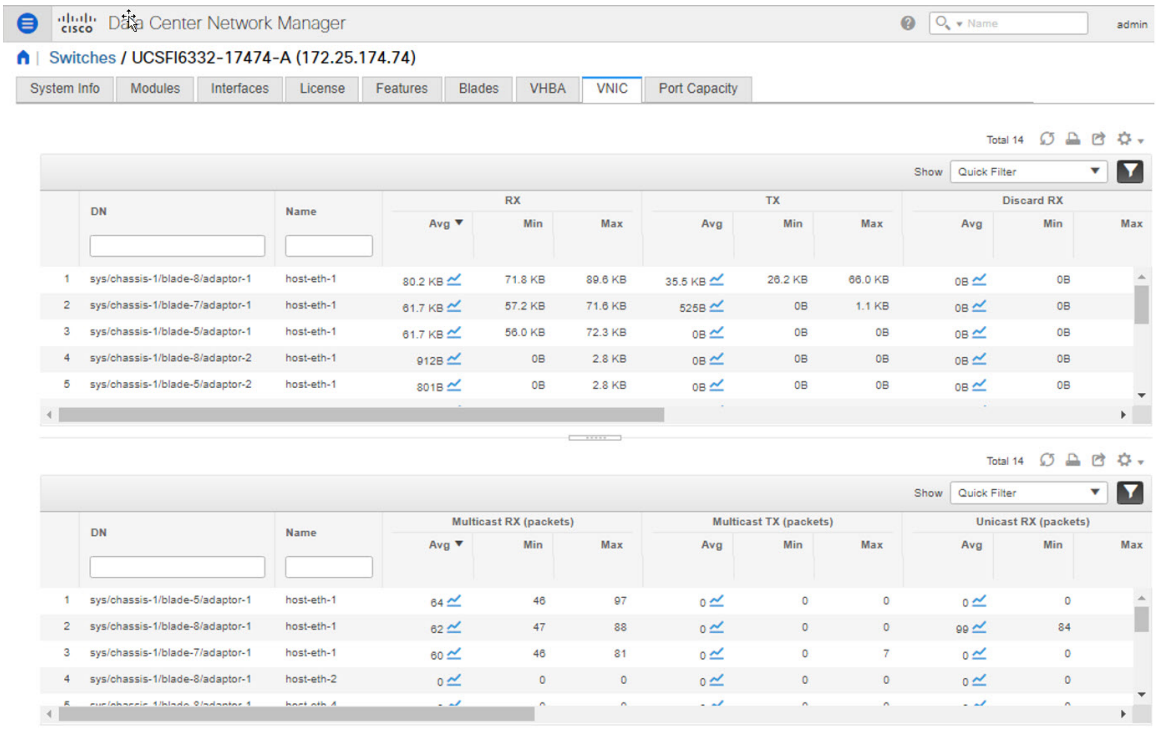
Blade	sys/chassis-1/blade-1	sys/chassis-1/blade-2	sys/chassis-1/blade-3
Name			
IP Address	127.6.1.5, 127.5.1.5	127.6.1.7, 127.5.1.7	127.6.1.8, 127.5.1.8
Description			
Admin Power	policy	policy	policy
Admin State	in-service	in-service	in-service
Assigned to Destination	org-root/ls-ucsb-n5k-rhel7	org-root/ls-ucsb-n5k-win2K12R2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

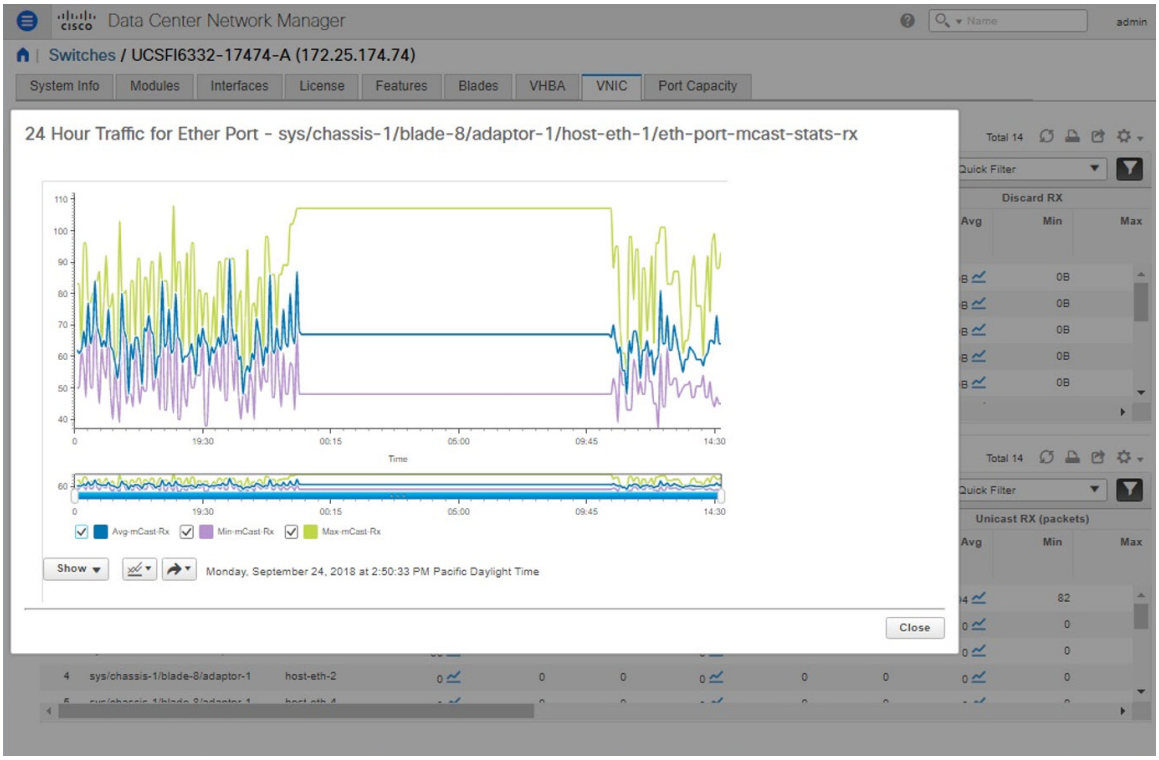
[vHBA] タブには、その特定の UCS FI の vHBA のリストが表示されます。グラフアイコンをクリックして、vHBA の 24 時間のトラフィックを表示します。





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


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

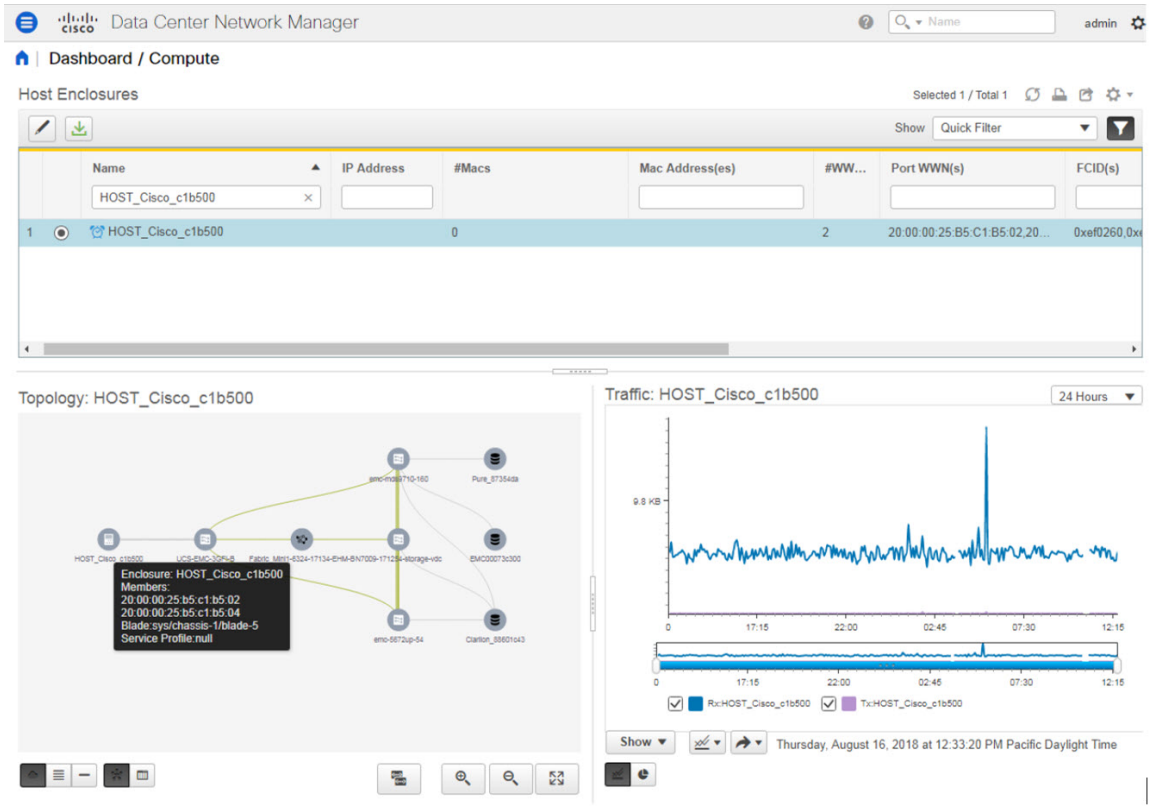

Data Center Network Manager
admin
Switches / UCSFI6332-17474-A (172.25.174.74)
System Info
Modules
Interfaces
License
Features
Blades
VHBA
VNIC
Port Capacity
24 Hour Traffic for Ether Port - sys/chassis-1/blade-8/adaptor-1/host-eth-1/eth-port-mcast-stats-rx
110
100
90
80
70
60
50
40
0
19:30
00:15
05:00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

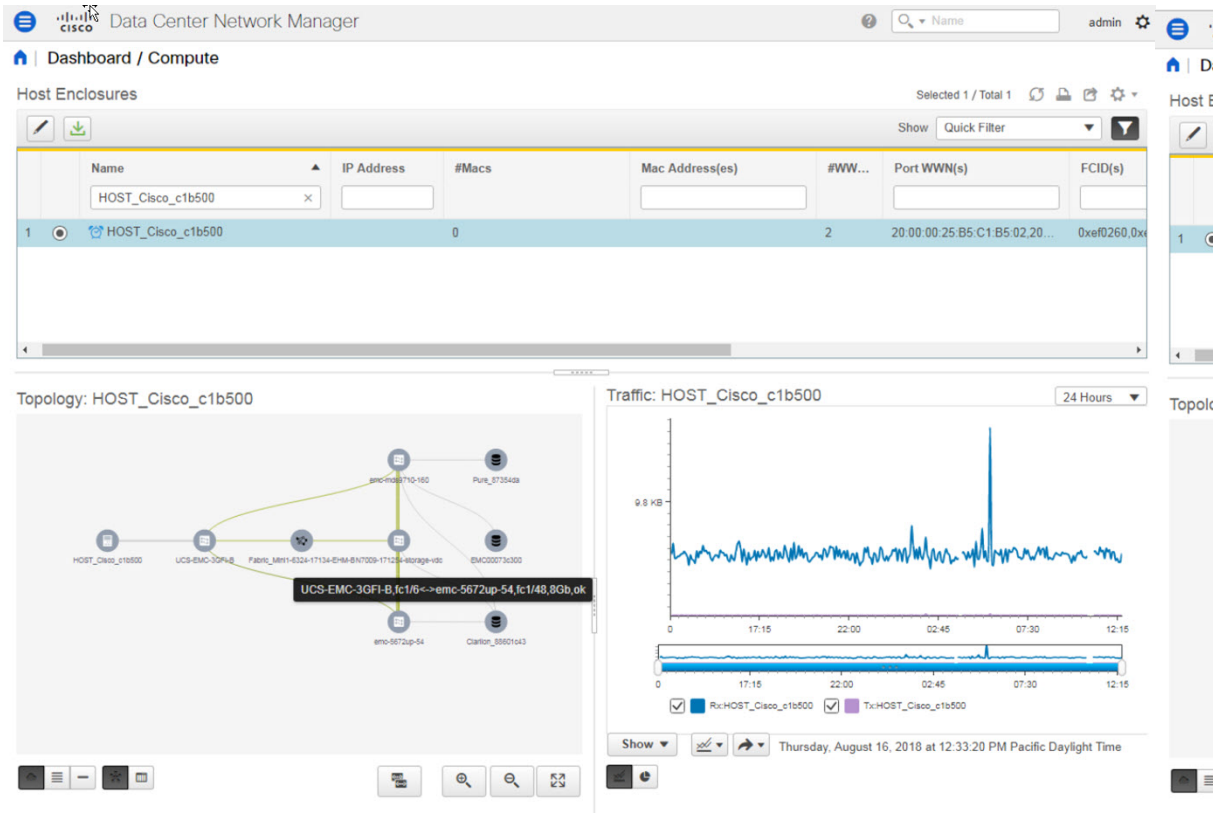
コンピューティング ダッシュボードで UCS FI 情報を表示

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

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

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





SMI-S ストレージの追加、編集、削除、再検出、更新

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

この項の内容は、次のとおりです。

SMI-S プロバイダーの追加

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

Procedure

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

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

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

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

ステップ 3 ドロップダウン リストを使用して、**[ベンダー（Vendor）]** を選択します。

サポートされているすべてのベンダーがドロップダウンリストに表示されます。ドロップダウンの **[その他（Other）]** のベンダーオプションを使用して、「ベストエフォート」ハンドラーを通じて、より多くの SMI-S ストレージベンダーが検出されます。

Note SMS-S ストレージ検出用のデータ ソースを追加する前に、1 つの有効な DCNM ライセンスをプロビジョニングする必要があります。

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

ステップ 5 **名前空間**と**相互運用名前空間**を指定します。

ステップ 6 デフォルトでは、**ポート**番号は事前に入力されています。

[セキュア（Secure）] チェックボックスをオンにすると、デフォルトのセキュアポート番号が入力されます。

EMC で**セキュア**モードを使用する場合、デフォルト設定は相互認証です。詳細については、トラストストアへの SSL 証明書の追加に関する EMC のドキュメントを参照してください。また、*Security_Settings.xml* 構成ファイルで SSLClientAuthentication 値を *None* に設定し、ECOM サービスを再起動することもできます。

ステップ 7 [Add] をクリックします。

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

SMI-S プロバイダーの削除

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

Procedure

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

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

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

SMI-S プロバイダの編集

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

Procedure

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

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

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

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

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

ステップ 6 デフォルトでは、**ポート**番号が事前入力されています。

[セキュア（Secure）] チェックボックスをオンにすると、デフォルトのセキュアポート番号が入力されます。

ステップ 7 **[適用 (Apply)]** をクリックします。

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

SMI-S プロバイダの再検出

Procedure

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

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

SMI-S プロバイダを消去

Procedure

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

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

プロバイダがパージされます。

VMware サーバの追加、編集、再検出、削除

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

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

この項の内容は、次のとおりです。

VirtualCenter サーバーを追加

Cisco DCNM から仮想センター サーバを追加できます。

Procedure

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

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

ステップ 2 [追加] をクリックします。

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

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

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

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

VMware サーバを削除

Cisco DCNM から VMware サーバを削除できます。

Procedure

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

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

VMware サーバーの編集

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

Procedure

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

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

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

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

ステップ 4 管理対象または管理対象外のステータスを選択します。

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

VMware サーバの再検出

Cisco DCNM から VMware サーバを再検出できます。

Procedure

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

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

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

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

ステップ 4 ダイアログ ボックスで [OK] をクリックします。

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。