



SAN ファブリック、リリース 12.1.3 について

目次

新機能と更新情報.....	1
ファブリック サマリ	2
ファブリック	3
ファブリックの追加.....	5
無差別モードの ESXi ネットワーキング.....	8
ファブリックの編集.....	10
ファブリックを削除しています.....	11
ファブリックの再検出.....	12
ファブリックのパーシ.....	13
パフォーマンスの設定	14
著作権	15

新機能と更新情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.1.3	再編成されたコンテンツ	このドキュメントの内容は、『Cisco NDFC-Fabric Controller Configuration Guide』または『Cisco NDFC-SAN Controller Configuration Guide』で提供されたものです。 リリース 12.1.3 以降、このコンテンツはこのドキュメントでのみ提供され、これらのドキュメントでは提供されなくなりました。

ファブリック サマリ

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

- **正常性**：ファブリックの正常性を示します。
- **アラーム**：カテゴリに基づいてアラームを表示します。
- **ファブリック情報**：ファブリックに関する基本情報を提供します。
- **インベントリ**：このセクションでは、スイッチの構成とスイッチの正常性に関する情報を提供します。

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

ファブリック

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

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

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

次の表では、[アクション (Actions)] メニューのドロップダウン リストにある、SAN > [ファブリック (Fabrics)] > [ファブリック (Fabrics)] で表示されます。

アクション項目	説明
ファブリックの追加	[アクション (Actions)] ドロップダウン リストで、[ファブリックの追加 (Add Fabric)] を選択します。詳細については、「 インスタンスの追加 」を参照してください。
ファブリックの編集	編集するファブリックを選択します。[アクション (Actions)] ドロップダウン リストで、[ファブリックの編集 (Edit Fabrics)] を選択します。必要な変更を行って、[適用 (Apply)] をクリックします。詳細な手順については、「 ファブリックの編集 」を参照してください。

アクション項目	説明
ファブリックの削除	削除する 1 つ以上のファブリックを選択します。 【アクション (Actions)】 ドロップダウンリストで、 【ファブリックの削除 (Delete Fabrics)】 を選択します。 【確認 (Confirm)】 をクリックして、ファブリックを削除します。詳細な手順については、「 ファブリックの削除 」を参照してください。
ファブリックの再検出	ファブリックに関連付けられたスイッチ、リンク、およびエンド デバイスを再検出できます。再検出する 1 つ以上のファブリックを選択します。 【アクション (Actions)】 ドロップダウンリストで、 【ファブリックの再検出 (Rediscover Fabrics)】 を選択します。 【状態 (State)】 列の進捗バーに、再検出の進行状況が表示されます。詳細な手順については、「 ファブリック の編集 」を参照してください。
ファブリックのパージ	ファブリックの存在しないスイッチ、リンク、およびエンド デバイスをパージできます。消去する 1 つ以上のファブリックを選択します。 【アクション (Actions)】 ドロップダウンリストで、 【ファブリックのパージ (Purge Fabrics)】 を選択します。詳細な手順については、「 ファブリックのパージ 」を参照してください。
パフォーマンスの設定	ファブリックに関連付けられたリンク、スイッチ インターフェイス、およびエンドデバイスのパフォーマンスモニタリングを有効にすることができます。パフォーマンスモニタリング用に 1 つ以上のファブリックを選択します。 【アクション (Actions)】 ドロップダウンリストで、 【パフォーマンスの構成 (Configure Performance)】 を選択します。必要な変更を行って、 【適用 (Apply)】 をクリックします。詳細な手順については、「 パフォーマンスの設定 」を参照してください。
SAN Insights の設定	選択したファブリックで SAN Insights を設定できます。詳細については、「 SAN Insights の構成 」を参照してください。
バックアップの設定	ファブリックデータのバックアップを設定およびスケジュールできます。詳細な手順については、『 NDFC Fabric Controller Configuration Guide 』の「バックアップと復元」を参照してください。

ファブリックの追加

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

1. [SAN]>[ファブリック (Fabrics)]>[SAN ファブリック (SAN Fabrics)] を選択します。
2. [アクション (Actions)]>[ファブリックの追加 (Add Fabrics)] を選択します。
3. [ファブリック名 (Fabric Name)] フィールドに一意のファブリック名を入力します。
4. [ファブリック シード スイッチ タイプ (Fabric Seed Switch Type)] を選択します。

リリース 12.1.2e 以降、NDFC を使用すると、SAN ファブリックに対する **Cisco** および **Cisco 以外** のスイッチを検出できます。

5. ファブリック シード スイッチ タイプで **Cisco** を選択した場合は、次の手順を実行します。
 - a. [ファブリック シード スイッチ (Fabric Seed Switch)] テキストボックスにシードスイッチの IP アドレスを入力します。

シードスイッチの DNS 名を入力することもできます。
 - b. アクセスを有効にするには、**SNMPv3/SSH** チェックボックスをオンにします。
 - c. [認証/プライバシー (Authentication/Privacy)] ドロップダウンリストから、スイッチの検出に適切な認証を選択します。
 - d. シードスイッチにアクセスするためのユーザー名とパスワードを適切なフィールドに入力します。



SNMPv3/SSH を使用しない場合は、
[コミュニティ文字列 (Community String)] フィールドに適切なコミュニティ文字列を入力します。

- e. VSAN のみを使用してスイッチを検出するには、[VSAN による検出の制限 (Limit Discovery by VSAN)] チェックボックスをオンにします。
 - VSAN に含まれるスイッチを検出するには、[含まれる VSAN リスト (Included VSAN List)] を選択します。
 - VSAN で除外されたスイッチを検出するには、[除外された VSAN リスト (Excluded VSAN List)] を選択します。
 - [VSAN リスト (VSAN List)] フィールドに、含める VSAN または除外する VSAN を入力します。
- f. UCS ログイン情報を使用してスイッチを検出するには、[UCS ログイン情報の使用 (Use UCS Credentials)] チェックボックスをオンにします。
 - [ユーザー名 (Username)] および [パスワード (Password)] フィールドに、UCS CLI ログイン情報を入力します。
 - 同じ SNMP ログイン情報を使用するには、[UCS に同じ SNMP ログイン情報を使用する (Use same SNMP Credentials for UCS)] チェックボックスをオンにします。

このチェックボックスをオフにする場合は、別の SNMP の詳細を指定する必要があります。

==

- UCS の SNMP を使用するには、[UCS に SNMPv3 を使用する (Use SNMPv3 for UCS)] チェックボックスをオンにします。
- SNMPv3 が使用されている場合、シードスイッチにアクセスするための[ユーザー名]と[パスワード]を適切なフィールドに入力します。



SNMPv3/SSH を使用しない場合は、
[UCS SNMP コミュニティ文字列 (Community String)] フィールドに適切な
コミュニティ文字列を入力します。

- SNMPv3 を使用しない場合は、[UCS SNMP コミュニティ文字列 (UCS SNMP Community String)] フィールドに適切なコミュニティ文字列を入力します。

6. [ファブリック シードスイッチ タイプ (Fabric Seed Switch Type)] で [Cisco 以外 (Non-Cisco)] を選択した場合は、次の手順を実行します。

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

シードスイッチの DNS 名を入力することもできます。

- b. アクセスを有効にするには、SNMPv3/SSH チェックボックスをオンにします。
- c. [認証/プライバシー (Authentication/Privacy)] ドロップダウンリストから、スイッチの検出に適切な認証を選択します。
- d. シードスイッチにアクセスするための[ユーザー名]と[パスワード]を適切なフィールドに入力します。
- e. [Cisco 以外のスイッチの CLI ログイン情報 (Non-Cisco Switch CLI Credentials)] で、Cisco 以外のシードスイッチにアクセスするための適切なユーザー名とパスワードを入力します。
- f. UCS クレデンシャルを使用してスイッチを検出するには、[UCS ログイン情報を使用する (Use UCS Credentials)] チェックボックスをオンにします。

- [ユーザー名 (Username)] および [パスワード (Password)] フィールドに、UCS CLI ログイン情報を入力します。
- 同じ SNMP ログイン情報を使用するには、[UCS に同じ SNMP ログイン情報を使用する (Use same SNMP Credentials for UCS)] チェックボックスをオンにします。

このチェックボックスをオフにする場合は、別の SNMP の詳細を指定する必要があります。

- UCS の SNMP を使用するには、[UCS に SNMPv3 を使用する (Use SNMPv3 for UCS)] チェックボックスをオンにします。

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

CS SNMP のユーザー名とパスワードを該当するフィールドに入力します。

- [UCS に SNMPv3 を使用する (Use SNMPv3 for UCS)] がオフの場合は、[UCS SNMP コミュニティストリング (UCS SNMP Community String)] フィールドに適切なコミュニティストリングを入力します。

7. [追加 (Add)] をクリックして、ファブリックを追加します。



SAN ファブリック検出を開始すると、ファブリック検出の 15 分後に、次のプロセスが NDFC でスケジュールされます。

ファブリックにライセンスがある場合は、Performance Manager (PM) 収集が開始されます。

- 。輻輳分析ジョブは、1 年間継続的に実行するようにスケジュールされています。このジョブの実行は、スケジュールの 1 時間後に開始されます。

無差別モードの ESXi ネットワーキング

Cisco NDFC Release 12.1.2e 以降、NDFC を仮想 Nexus Dashboard (vND) インスタンス上で実行するには、外部サービス IP アドレスが指定されている Nexus Dashboard インターフェイスに関連付けられているポートグループで無差別モードを有効にする必要があります。vND は、Nexus Dashboard 管理インターフェイスとデータインターフェイスで構成されています。デフォルトでは、ファブリック コントローラ ペルソナで、Nexus Dashboard 管理インターフェイス サブネットに 2 つの外部サービス IP アドレスが必要です。

NDFC リリース 12.1.2e の前に、インバンド管理、エンドポイント ロケータ、または POAP 機能が NDFC で有効になっている場合、Nexus Dashboard データまたはファブリック インターフェイス ポート グループに対して無差別モードを有効にする必要もありました。この設定は、これらの機能に関連付けられているトラフィック フローには必須でした。

無差別モードを有効にすると、NDFC のセキュリティ問題のリスクが高まります。無差別モードのデフォルト設定を設定することをお勧めします。

に

- 無差別モードの無効化は、Cisco Nexus Dashboard リリース 2.3.1c からサポートされています。
- Nexus Dashboard ノードがデータ ネットワーク上でレイヤ 3 隣接し、BGP が構成されており、データ インターフェイスを介してファブリック スイッチに到達できる場合は、無差別モードを無効にすることができます。
- Nexus Dashboard インターフェイスがスイッチ mgmt0 インターフェイスにレイヤ 2 に隣接している場合、無差別モードをディセーブルにできます。

インバンド管理または EPL が有効になっている場合は、Nexus Dashboard データ インターフェイス サブネットで外部サービス IP アドレスを指定する必要があります。また、Nexus Dashboard のデータ/ファブリック インターフェイス ポート グループに対して、無差別モードを無効にすることができます。詳細については、『Cisco Nexus Dashboard Fabric Controller Deployment Guide』を参照してください。



無差別モードのデフォルトオプションは **[拒否 (Reject)]** です。

1. **vSphere** クライアントにログインします。
2. ESXi ホストに移動します。
3. ホストを右クリックし、**[Settings (設定)]** を選択します。

サブメニューが表示されます。

4. **[ネットワーキング (Networking)]** > **[仮想スイッチ (Virtual Switches)]** を選択します。

すべての仮想スイッチがブロックとして表示されます。

5. VM ネットワークの **[設定を編集 (Edit Settings)]** をクリックします。
6. **[セキュリティ (Security)]** タブに移動します。
7. 無差別モードの設定を次のように更新します。

- **[オーバーライド (Override)]** チェックボックスをオンにします。

- ドロップダウン リストから **【承認 (Accept)】** を選択します。

8. **【OK】** をクリックします。

ファブリックの編集

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

1. **[SAN]>[ファブリック (Fabrics)]>[SAN ファブリック (SAN Fabrics)]**を選択します。
2. チェックボックスをオンにして、必要なファブリック名を編集し、**[アクション (Actions)]>[ファブリックの編集 (Edit Fabrics)]**を選択します。
3. **[ファブリックの編集 (Edit Fabrics)]** ウィンドウでは、一度に 1 つのファブリックのみを編集できます。
4. 新しいファブリックの **[ファブリック名 (Fabric Name)]**を入力します。
5. (オプション) **[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。
6. **[ユーザー名 (Username)]**と **[パスワード (Password)]**、プライバシーを入力し、いずれかのステータス オプションを選択することで、SAN コントローラ Web クライアントでファブリックを管理する方法を指定します。
7. ステータスを **[管理 (Managed)]**、**[非管理 (Unmanaged)]**、または **[継続的に管理 (Managed Continuously)]**に変更します。
8. (オプション) UCS ログイン情報を変更する場合は、**[UCS ログイン情報を使用する (Use UCS Credentials)]**チェックボックスをオンにします。
9. ユーザー名とパスワードを入力します。
10. **[適用 (Apply)]**をクリックして、変更内容を保存します。

ファブリックを削除しています

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

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

ファブリックの再検出

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

1. **[SAN]>[ファブリック (Fabrics)]>[SAN ファブリック (SAN Fabrics)]** を選択します。
2. チェックボックスを選択して必要なファブリック名を再検出し、**[アクション (Actions)]>[ファブリックの再検出 (Rediscover Fabrics)]** を選択します。
3. ダイアログボックスで **[はい (Yes)]** をクリックします。

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

ファブリックのパージ

[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。

1. [SAN]>[ファブリック (Fabrics)]を選択します。
2. パージ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。
3. [アクション (Actions)] [ファブリックのパージ (Purge Fabrics)] を選択します。

ファブリックはパージされます。

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

- [トポロジ (Topology)] を選択し、ファブリックを選択し、ファブリックを右クリックして、[ファブリックをパージする (Purge Down Fabric)] を選択します。

ファブリックはパージされます。

パフォーマンスの設定

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

1. **[SAN]>[ファブリック (Fabrics)]**を選択します。
2. パフォーマンス収集を設定するファブリックの横にあるチェックボックスをオンにします。
3. **[アクション (Actions)]** **[パフォーマンスの構成 (Configure Performance)]** を選択します。

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

4. 他のチェックボックスを有効にするには、**[パフォーマンス収集 (Performance Collection)]** チェックボックスをオンにします。
5. 必要な **ISL/NPV** リンク、ホスト、ストレージ、および **FC** イーサネットを選択するか、**[すべて選択 (Select All)]** ボックスを選択して、これらのデータ タイプのパフォーマンス収集を有効にします。
 - a. SAN デバイスの温度データを収集するには、**[設定 (Settings)]>[サーバー設定 (Server Settings)]>[PM]** を選択します。
 - b. **[PM]** タブで、**[SAN センサー検出を有効にする (Enable SAN Sensor Discovery)]** および **[SAN スwitchの温度を収集する (Collect Temperature for SAN Switches)]** のチェックボックスをオンにします。
6. **[適用 (Apply)]** をクリックして、設定を保存します。
7. 確認ダイアログボックスで、**[はい (Yes)]** をクリックしてパフォーマンス コレクタを再起動します。

次に行う作業：

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

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

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

シスコおよびシスコのロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、<http://www.cisco.com/go/trademarks> を参照してください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)。

© 2017-2023 Cisco Systems, Inc. All rights reserved.