



Cisco Nexus Dashboard ファブリック クの管理、リリース 3.2.x

目次

ファブリックの正常性.....	2
ACI ファブリックの追加	3
NDFC ファブリックの追加.....	5
NX-OS スイッチ（コントローラなし）の追加	7
ファブリックの編集	8
ファブリックの削除	9
商標	10

Cisco Nexus Dashboard を使用して、複数の Cisco ACI、Cisco Cloud Network Controller、Cisco NDFC ファブリック、および NX-OS スイッチ（コントローラなし）を「ファブリック」として同じクラスタにオンボードできます。ファブリックがオンボードされると、同じCisco Nexus Dashboardクラスタで実行されているアプリケーションで使用できるようになります。

ファブリックを追加するには、そのコントローラのインバンドまたはアウトオブバンドの IP アドレスとログイン情報が必要です。ファブリックのオンボーディングに使用するIPアドレスのタイプは、ファブリックを使用するNexus Dashboard サービスによって異なります。詳細については、次のセクションで説明します。Cisco Nexus Dashboard クラスタに追加されたファブリックは、デフォルトではサービスで有効化されていないため、各サービスの GUI から直接明示的に有効化する必要があります。

Nexus Dashboard に 1 つ以上のファブリックをオンボードした後、左側のナビゲーション サイドバーから **[ファブリック (Fabrics)]** を選択すると、オンボードしたサイトを Nexus Dashboard GUI で表示できます。**[ファブリック (Fabrics)]** ページでファブリック名の横にある **[開く (Open)]** リンクをクリックして、ファブリックの GUI を直接起動することもできます。

リモート認証を使用して Nexus Dashboard にログインし、起動するファブリックで同じログインドメインとユーザーが構成されている場合は、再認証することなくファブリックの GUI に自動的にログインできます。

ファブリックの正常性

次のセクションの説明に従ってファブリックを追加したら、

Nexus Dashboard 管理コンソールの [管理 (Manage)] > [ファブリック (Fabrics)] ページにあるステータスを表示できます。

ファブリックの [名前 (Name)] に加えて、各ファブリックについて次の情報を確認できます。

■ ヘルス スコア

- [正常 (Healthy)] : ファブリックの正常性スコアが 90 以上の場合。
- [警告 (Validating Peer Certificates)] : ファブリックの正常性スコアが 76 ~ 89 の場合。
- [マイナー (Minor)] : ファブリックの正常性スコアが 50 ~ 75 の場合。
- [主要 (Major)] : ファブリックの正常性スコアが 25 ~ 49 の場合。
- [重大 (Critical)] : ファブリックの正常性スコアが 25 未満の場合。

■ Type

- Cisco APIC によって管理されるファブリックの **ACI**
- Cisco NDFC によって管理されるファブリックの **NDFC**
- **スタンドアロン NX-OS スイッチの NX-OS** スイッチ (コントローラなし)

- [接続ステータス (Connectivity Status)] : ファブリックが Nexus Dashboard クラスタから到達可能かどうかを示します。

- [ファームウェアバージョン (Firmware Version)] : ファブリックのコントローラまたはスイッチで実行されているソフトウェアのバージョン。

Manage > Fabrics

Fabrics Refresh

Filter by attributes Add Fabric

Health Score	Name	Type	Connectivity Status	Firmware Version	Enabled Services
 Major	fab1	 NDFC	 Up	12.2.2.214	1 ...

1 items found Rows per page 10 < 1 >

ACI ファブリックの追加

はじめる前に

- ファブリック接続がすでに設定されている必要があります。
- サービスと互換性のある特定のファブリック バージョンの場合、「[サービス互換性マトリクス](#)」を参照してください。
- Cisco APIC ファブリックを追加する場合は、Cisco Nexus Dashboard データ ネットワークの IP 接続用の EPG/L3Out を事前に構成する必要があります。

詳細については、「[ファブリック接続](#)」を参照してください。

- Cisco APIC ファブリックを追加し、Insights サービスのインストールを計画している場合は、次のステップを実行します。
 - Cisco Nexus Dashboardからデータネットワークを介したCisco APICインバンドIPへのIP接続を設定する必要があります。
 - Cisco Nexus DashboardからリーフノードおよびスパインノードのインバンドIPへのIP接続を設定する必要があります。

ACI ファブリックを追加するには、次のステップを実行します。

1. Nexus Dashboard の **[管理コンソール (Admin Console)]** に移動します。
2. メインメニューで、**[管理 (Manage)]** > **[ファブリック (Fabrics)]** を選択します。
3. メインペインで、**[ファブリックの追加 (Add Fabric)]** をクリックします。**[ファブリックの追加 (Add Fabric)]** 画面が開きます。
4. **[ファブリックの追加 (Add Fabric)]** ページで、ファブリックの情報を入力します。
 - **[ホスト名/IP アドレス (Host Name/IP Address)]** : ファブリックのコントローラとの通信に使用する IP アドレスを入力します。
 - **[ユーザー名 (User Name)]** と **[パスワード (Password)]** : 追加するファブリックで**管理者権限**を持つユーザーのログインクレデンシャル。
 - (オプション) **[ログイン ドメイン (Login Domain)]** : このフィールドを空白にすると、ファブリックのローカルログインが使用されます。
 - (オプション) **[ピア証明書を検証 (Validate Peer Certificate)]** : Nexus Dashboard が、接続先ホスト (例えばファブリック コントローラ) の証明書が有効であることと、信頼されている認証局 (CA) に署名されていることを検証できるようにします。



このオプションを使用してファブリックを追加する前に、このファブリックの証明書を Nexus Dashboard にインポートしておく必要があります。証明書をまだ追加していない場合は、**[ファブリックの追加 (Add Fabric)]** ウィザードをキャンセルし、最初に **[ピア証明書の検証 (Validating Peer Certificates)]** で説明されている手順に従ってください。その後、証明書をインポートしてから、ここで説明するようにファブリックを追加します。有効な証明書をインポートせずに **[ピア証明書を検証 (Verify Peer Certificate)]** オプションを有効にするとファブリックの導入準備は機能不全になります。

必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。

5. **[詳細 (Detail)]** ページで、追加のファブリックの詳細を入力します。

- **[名前 (Name)]** : ファブリックの説明的な名前。

- **[場所 (Location)]** : サイトの地理的な場所。このオプションは、オンプレミス ファブリックでのみ使用できます。必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。

6. **[概要 (Summary)]** ページで情報を確認し、**[保存 (Save)]** をクリックしてファブリックの追加を完了します。

NDFC ファブリックの追加

はじめる前に

- ファブリック接続がすでに設定されている必要があります。
- サービスと互換性のある特定のファブリック バージョンの場合、「[サービス互換性マトリクス](#)」を参照してください。
- Cisco NDFC ファブリックを追加する場合：
 - ファブリックとスイッチへのレイヤ3接続を設定する必要があります。
 - クラスタがAWSまたはAzureに展開されている場合は、データインターフェイスでインバウンドルールを設定する必要があります。

これは通常、最初のクラスタ展開中に行われ、「Cisco Nexus Dashboard Deployment Guide」で詳細に説明されています。

NDFC ファブリックを追加するには、次のステップを実行します。

1. Nexus Dashboard の **[管理コンソール (Admin Console)]** に移動します。
2. メインメニューで、**[管理 (Manage)] > [ファブリック (Fabrics)]** を選択します。
3. メインペインで、**[ファブリックの**

追加 (Add Fabric)] をクリックしま

す。**[ファブリックの追加 (Add**

Fabric)] 画面が開きます。

4. **[ファブリックの追加 (Add Fabric)]** ページで、ファブリックの情報を入力します。

- **[ホスト名/IP アドレス (Host Name/IP Address)]** : ファブリックのコントローラとの通信に使用する IP アドレスを入力します。



NDFC ファブリックの場合、これは NDFC のインバンド IP アドレスである必要があります。アドレスを指定する場合、URL 文字列の一部としてプロトコル ([http://](#) または [https://](#)) を含めないでください。追加すると、ファブリックの追加に失敗します。

- **[ユーザー名 (User Name)]** と **[パスワード (Password)]** : 追加するファブリックで **管理者権限** を持つユーザーのログインクレデンシャル。
- (オプション) **[ログインドメイン (Login Domain)]** : このフィールドを空白にすると、ファブリックのローカルログインが使用されます。
- (オプション) **[ピア証明書を検証 (Validate Peer Certificate)]** : Nexus Dashboard が、接続先ホスト (例えばファブリック コントローラ) の証明書が有効であることと、信頼されている認証局 (CA) に署名されていることを検証できるようにします。



このオプションを使用してファブリックを追加する前に、このファブリックの証明書を Nexus Dashboard にインポートしておく必要があります。証明書をまだ追加していない場合は、**[ファブリックの追加 (Add Fabric)]** ウィザードをキャンセルし、最初に **[ピア証明書の検証 (Validating Peer Certificates)]** で説明されている手順に従ってください。その後、証明書をインポートしてから、ここで説明するようにファブリックを追加します。

有効な証明書をインポートせずに **[ピア証明書を検証 (Verify Peer Certificate)]** オプションを有効にするとファブリックの導入準備は機能不全になります。

必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。

5. **[詳細 (Detail)]** ページで、追加のファブリックの詳細を入力します。

- **[名前 (Name)]** : ファブリックの説明的な名前。
- **[場所 (Location)]** : サイトの地理的な場所。このオプションは、オンプレミス ファブリックでのみ使用できます。

必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。

6. **[概要 (Summary)]** ページで情報を確認し、**[保存 (Save)]** をクリックしてファブリックの追加を完了します。

NX-OS スイッチ（コントローラなし）の追加

はじめる前に

- シードスイッチへの接続は、すでに構成されている必要があります。シードスイッチはファブリックのその他のスイッチを検出するために使用されます。
- コントローラ（APIC や NDFC など）のない NX-OS スイッチは、Nexus Dashboard Insights サービスでのみサポートされます。
- NDI が NDFC または NDO と共存している場合、NX-OS の検出は使用できません。

NX-OS スイッチをファブリックとして追加するには、次のステップを実行します。

1. Nexus Dashboard の **[管理コンソール (Admin Console)]** に移動します。
2. メインメニューで、**[管理 (Manage)]** > **[ファブリック (Fabrics)]** を選択します。
3. メインペインで、**[ファブリックの追加 (Add Fabric)]** をクリックします。**[ファブリックの追加 (Add Fabric)]** 画面が開きます。
4. **[ファブリックの追加 (Add Fabric)]** 画面で、**[NX-OS スタンドアロンサイト (NX-OS Standalone Site)]** を選択します。



コントローラなしで NX-OS スイッチを初めてオンボーディングする場合は、**[ファブリック検出の有効化 (Enable Fabric Discovery)]** をクリックします。

5. **[ファブリックの追加 (Add Fabric)]** ページで、ファブリックの情報を入力します。
 - **[シードスイッチ IP アドレス (Seed Switch IP Address)]** : ファブリック内の他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の IP アドレスを指定します。
 - **[ユーザー名 (Username)]** と **[パスワード (Password)]** : シードスイッチのログインクレデンシャル。必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。
6. **[詳細 (Detail)]** ページで、追加のファブリックの詳細を入力します。
 - **[名前 (Name)]** : ファブリックの説明的な名前。
 - **[場所 (Location)]** : サイトの地理的な場所。このオプションは、オンプレミスファブリックでのみ使用できます。必要な情報を入力したら、**[次へ (Next)]** をクリックして続行します。
7. **[スイッチの選択 (Switch Selection)]** ページで、「ファブリック」として追加する 1 つ以上のスイッチを選択します。

スイッチ検出プロセスのデフォルトでは、シードスイッチから 2 ホップ離れたスイッチが表示されます。デフォルトの設定は、**[ホップ数 (Number of Hops)]** ドロップダウンを使用し、**[スイッチの再検**

出 (**Rediscover Switches**)] をクリックして変更できます。

スイッチが検出されたら、**Nexus Dashboard** にファブリックとして追加するすべてのスイッチを選択し、[次へ (**Next**)] をクリックします。

8. [概要 (**Summary**)] ページで情報を確認し、[保存 (**Save**)] をクリックしてファブリックの追加を完了します。

ファブリックの編集

ファブリックを編集するには、次のステップを実行します。

1. Nexus Dashboard の **[管理コンソール (Admin Console)]** に移動します。
2. メインメニューで、**[管理 (Manage)]** > **[ファブリック (Fabrics)]** を選択します。
3. 編集するサイトの **[アクション (Actions)]** (...) メニューから、**[ファブリックの編集 (Remove Site)]** を選択します。**[ファブリックの編集 (Edit Fabric)]** 画面が開きます。
4. **[ファブリックの編集 (Edit Fabric)]** 画面で必要な変更を加えます。
 - セキュリティドメインを削除するには、既存のドメインの横にある **[削除 (Delete)]** アイコンをクリックします。
 - 1 つ以上のセキュリティドメインを追加するには、**[+セキュリティドメインの追加 (+Add Security Domain)]** をクリックします。
 - ファブリックを再プロビジョニングするには、**[ファブリックの再登録 (Re-register Fabric)]** チェックボックスをオンにして、必要な情報を入力します。

Cloud Network Controller のパブリック IP アドレスが変更された場合、Nexus Dashboard Orchestrator で使用される Cloud Network Controller ファブリックでは、ファブリックの再登録が必要になる場合があります。

オーケストレータ サービスによって管理される NDFC ファブリックの IP アドレス情報を変更した場合にも、このオプションを使用できます。



Nexus Dashboard Insights サービスでは、ファブリックの再登録はサポートされていません。

Nexus Dashboard にファブリックを再登録した後、ファブリックを削除してから、Nexus Dashboard Insights にファブリックを再度追加する必要があります。保証は、ファブリックを再登録する前に収集されたデータでの実行に失敗します。

5. **[保存 (Save)]** をクリックして、変更内容を保存します。

ファブリックの削除

はじめる前に

- Nexus Dashboardにインストールされているアプリケーションでファブリックが使用されていないことを確認します。ファブリックを削除すると、このファブリックを使用しているすべてのアプリケーションが中断されます。
- Cisco ACI ファブリックがファブリックとして Nexus Dashboard に追加されている場合、いくつかのポリシーが Cisco APIC で作成されている可能性があります。オンボードされているファブリックを削除することなく Nexus Dashboard をクリーンリブートしても、Cisco APIC で作成されたポリシーは削除されません。Cisco APIC でこれらのポリシーをクリーンアップするには、ファブリックを再度追加して削除する必要があります。

1つまたは複数のファブリックを削除するには、次のステップを実行します。

1. Nexus Dashboard の **[管理コンソール (Admin Console)]** に移動します。
2. メインメニューで、**[管理 (Manage)]** > **[ファブリック (Fabrics)]** を選択します。
3. 削除するサイトの **[アクション (Actions)]** (...) メニューから、**[ファブリックの削除 (Remove Site)]** を選択します。
4. **[削除の確認 (Confirm Delete)]** ウィンドウに、ファブリックのログイン情報を入力します。
5. **[OK]** をクリックして、ファブリックを削除します。

商標

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』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している 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。

Cisco および Cisco のロゴは、Cisco 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。

商標または登録商標です。Cisco の商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認いただけます。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)。

© 2017-2024 Cisco Systems, Inc. All rights reserved.

初版：2024 年 3 月 1 日

最終更新日：2024 年 3 月 1 日

米国本社

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax : 408 527-0883