SAN 動作用スイッチの追加モードのインターフェイスの追加モード、リリース 12.1.3

目次

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または、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。
NDFC リリース 12.1.3	実行 CLI 機能の拡張。	CLI の実行機能が拡張され、[セッション タイムアウト（Session Timeout）] フィールドが追加され、CLI コマンドをスイッチで実行したり、CLI の実行出力を表示したりするための追加オプションが提供されるようになりました。

スイッチ

次の表で、**[スイッチ（Switches）]**ウィンドウに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
スイッチ名	スイッチの名前を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
Fabric Name（ファブリック名）	スイッチに関連付けられているファブリック名を指定します。
ステータス	スイッチのステータスを指定します。
ヘルス（Health）	スイッチの正常性ステータスを指定します。正常性ステータスは次のとおりです。 • 正常 • 深刻 • 警告 • OK
Ports	スイッチのポートの合計数を指定します。
使用済みポート	スイッチで使用されるポートの合計数を指定します。
モデル	スイッチ モデルを指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。
リリース	スイッチのリリース番号を指定します。
稼働時間	スイッチアップ時間の詳細を指定します。

次のテーブルでは、[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 > [スイッチ（Switches）] > [スイッチ（Switches）] で表示されるアクション項目が説明されています。**

アクション項目	説明
Device Manager	必要なスイッチのデバイスマネージャにログインできます。**[デバイス マネージャ**のログイン（Device Manager login）] ウィンドウが表示され、ログイン情報を入力してログインします。Cisco MDS 9000 デバイス マネージャの使用方法の説明と手順については、「デバイス マネージャ（Device Manager ）」を参照してください。
テクニカル サポート	ログの収集を開始できます。詳細については、「テクニカルサポート（Tech Support）」を参照してください
CLI の実行	複数のスイッチで複数の CLI コマンドを実行し、各スイッチの出力を zip 形式のテキストファイルとして収集できます。詳細については、「CLI の実行」を参照してください。
Brocade パラメータの移行	

Device Manager

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。

Cisco Nexus ダッシュボード ファブリック コントローラ リリース 12.1.3 以降では、スイッチ ダッシュボードで使用可能なデバイス マネージャ サービスに加えて、ローカル システムにスタンドアロンのデバイス マネージャ アプリケーションをダウンロードしてインストールできます。

デバイス マネージャのダウンロード

はじめる前に

クライアント コンピュータに Windows または Linux オペレーティング システムがインストールされている。

このセクションでは、デバイス マネージャをローカル システムにダウンロードする手順について説明します。

1. Cisco Nexus ダッシュボード ファブリック コントローラ内で **SAN > [スイッチ（Switches）]** を選択します。

   スイッチ ダッシュボードが表示されます。

2. **[アクション（More Actions）]** ドロップダウン リストから **[デバイス マネージャ（ Device Manager）]** を選択します。

   これにより、デバイス マネージャ クライアント ファイルが *tar.gz* フォーマットでシステムにダウンロードされます。その後、アーカイブ ファイルを抽出してその内容を表示することができます。

3. インストールされているオペレーティング システムに応じて、スクリプトまたはバッチ ファイルを実行して、デバイス マネージャ アプリケーションをシステムにインストールします。

   Linux システムでは、スクリプト ファイル（*.sh）ファイルは /bin ディレクトリにあります。

   Windows システムでは、スクリプト ファイル（*.bat）ファイルは*/bin*

   *directory*にあります。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。

4. 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。

   システムは、デバイス マネージャをスタンドアロン アプリケーションとしてローカル システムにダウンロードします。

   Cisco MDS 9000 デバイス マネージャの説明と使用方法については、デバイス マネージャを参照してください。

テクニカル サポート

[アクション（Actions）] ドロップダウンリストから、**[テクニカル サポート**（Tech Support）] を選択してログ収集を開始します。ウィンドウが表示されます。

- **[セッションタイムアウト（Session timeout）]** フィールドに時間を分単位で入力します。デフォルトの時間は 20 分です。
- **[コマンド（Command）]** テキストフィールドにコマンドを入力し、**[実行（Run）]** をクリックします。
- [データが正常に送信され、テクニカルサポートが開始されました（Data submitted successfully, tech support starting）] という確認ウィンドウが表示され、**[確認（Confirm）]** をクリックしてステータスが **[完了（Completed）]** に変わります。
- レポートをダウンロードするには、**[テクニカルサポートのダウンロード（Download Tech Support）]** をクリックします。

CLI の実行

Cisco NDFC SAN コントローラを使用すると、スイッチで CLI コマンドを実行できます。各スイッチの zip ファイル内の CLI コマンドからの出力を収集できます。

スイッチで CLI コマンドを実行するには、次の手順を実行します。

1. Cisco NDFC UI で、**[SAN] > [スイッチ（Switches）]** を選択します。
2. CLI コマンドを実行するスイッチを選択します。

   複数のスイッチを選択して、一連の CLI コマンドを同時に実行できます。

3. **[アクション（Actions）]** ドロップダウンリストから、

   [CLI の実行（Execute CLI）] を選択します。**[スイッチ**

   CLI の実行（Execute Switch CLI）] 画面が表示されま

   す。

4. **[設定（Configure）]** タブで、**[選択されたスイッチ**（Selected Switches）] の下のハイパーリンクをクリックして、CLI が実行される選択されたスイッチを表示します。
5. **[セッション タイムアウト（Session Timeout）]** エリアで、セッション タイムアウトまでの時間を入力します。

   有効なオプションは 2 ～ 10 分です。デフォルト エントリは 5 分です。

6. スイッチで実行する CLI コマンドを提供する方法を決定します。

   - スイッチ上で実行する **CLI コマンド** を入力します。あるいは、
   - **[コマンドファイルの読み取り（Read Commands File）]** ボタンをクリックし、実行する CLI コマンドのリストを含む .txt 拡張子のファイルをアップロードします。

   [CLI コマンド] テキスト ボックスまたは .txt ファイルに、1 行に 1 つのコマンドを入力します。

7. **[実行（Execute）]** をクリックします。

   すべてのスイッチでコマンドの実行が完了すると、ポップアップウィンドウが表示され、**CLI の実行出力**が表示されます。

8. **[閉じる（Close）]** をクリックします。

   [スイッチ CLI を実行（Execute Switch CLI）] ウィンドウに戻り、テーブルにスイッチ、関連するファブリック、および CLI の実行ステータスが表示されます。

   - [**出力の表示**（Show Output）] をクリックすると、ポップアップ ウィンドウが再度表示され、CLI **の実行**出力が表示されます。

     出力が数 MB を超える場合、**show の出力**は切り捨てられます。その場合は、ファイルをダウンロードして完全な出力を表示する必要があります。 **出力の表示**は、ほとんど表示せずにデバッグを高速化するための簡単な出力を目的としており、ダウンロードされたファイルを使用して行われるオフライン デバッグには適していません。

- コマンド出力を zip ファイルとしてダウンロードするために**[出力のダウンロード（Download output）]** をクリックします。
- このウィンドウの手順が完了したら、**[完了（Done）]** をクリックします。

CLI 経由でスイッチに到達できない場合、zip ファイルの出力にエラーが表示されます。

拡張されたロールベースのアクセス制御

SAN コントローラリリース 12.0.1（a）からは、すべての RBAC が Nexus ダッシュボードにあります。ユーザロールとアクセスは、NDFC 上のファブリックの Nexus ダッシュボードから定義されます。

Nexus ダッシュボードの管理者ロールは、NDFC のネットワーク管理者ロールと見なされます。

DCNM には、さまざまなアクセスと操作を実行するための 5 つのロールがありました。ユーザーがアクセスする場合、ネットワークステージロールを持つファブリックは、ネットワークステージロールとして他のすべてのファブリックにアクセスできます。したがって、ユーザー名は DCNM でのロールによって制限されます。

Cisco NDFC リリース 12.0.1(a) には同じ 5 つのロールがありますが、Nexus ダッシュボードの統合により詳細な RBAC を実行できます。ユーザーがネットワークステージロールとしてファブリックにアクセスする場合、同じユーザーは、管理者またはオペレーターロールなどの他のユーザーロールを使用して別のファブリックにアクセスできます。したがって、ユーザーは NDFC のさまざまなファブリックでさまざまなアクセス権を持つことができます。

NDFC RBAC は、次のロールをサポートします。

- NDFC アクセス管理者
- NDFC デバイス アップグレード管理者
- NDFC ネットワーク管理者
- NDFC ネットワーク オペレータ
- NDFC ネットワーク ステージャ

次の表では、NDFC でのユーザーロールとその権限について説明します。

ロール	権限
NDFC アクセス管理者	読み取り/書き込み
NDFC デバイス アップグレード管理者	読み取り/書き込み
NDFC ネットワーク管理者	読み取り/書き込み
NDFC ネットワーク オペレータ	読み取り
NDFC ネットワーク ステージャ	読み取り/書き込み

DCNM では、下位互換性のために次のロールがサポートされています。

- SAN 管理者（ネットワーク管理者にマッピング）
- グローバル管理者 (ネットワーク管理者にマッピング)
- SAN ネットワーク管理者（ネットワーク管理者にマッピング）
- サーバー管理者（ネットワーク管理者にマッピング）

どのウィンドウでも、ログインしているユーザーロールで実行できないアクションはグレー表示されます。

NDFC ネットワーク管理者

NDFC ネットワーク管理者ロールを持つユーザーは、SAN コントローラですべての操作を実行できます。

Cisco Nexus ダッシュボード ファブリック コントローラ リリース 12.1.1e から、このロールを持つユーザーは、ネットワークおよび VRF の MSD ファブリックのすべての操作を実行できます。

NDFC ネットワーク管理者ロールを持つユーザーは、SAN コントローラの特定のファブリックまたはすべてのファブリックをフリーズできます。

> NDFC の検出または追加のスイッチまたは LAN ログイン情報のスイッチ ユーザー ロールに network-admin ロールがあることを確認してください。

NDFC デバイス アップグレード管理者

NDFC デバイス アップグレード管理者ロールを持つユーザーは、**[イメージ管理（Image Management）]** ウィンドウでのみ操作を実行できます。

詳細については、「イメージ管理」の項を参照してください。

NDFC アクセス管理者

NDFC アクセス管理者ロールを持つユーザーは、すべてのファブリックの**[インターフェイス マネージャ（Interface Manager）]**ー
ウィンドウでのみ操作を実行できます。

NDFC アクセス管理者は、次のアクションを実行できます。

- レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。
- ホスト vPC、およびイーサネット インターフェイスを編集します。
- 管理インターフェイスからの保存、プレビュー、および展開。
- LAN クラシックおよび IPFM ファブリックのインターフェイスを編集します。

  nve、管理、トンネル、サブインターフェイス、SVI、インターフェイス グループ、およびループバック インターフェイスを除く

ただし、SAN コントローラ アクセス ロールを持つユーザは、次のアクションを実行できません：

- レイヤ 3 ポート チャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。
- レイヤ 3、ST FEX、AA FEX のメンバー インターフェイスおよびポート チャネルは編集できません。
- Easy ファブリック用に、アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。
- ピア リンク ポート チャネルを編集できません。
- 管理インターフェイスを編集できません。
- トンネルを編集できません。

ファブリックまたは SAN コントローラが deployment-freeze モードの場合、このロールのアイコンとボタンはグレー表示されます。

NDFC ネットワーク ステージャ

NDFC ネットワーク ステージャ ロールを持つユーザーは、SAN コントローラで構成を変更できます。**NDFC ネットワーク管理者**ロールを持つユーザーは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

- インターフェイス構成の編集
- ポリシーの表示または編集
- インターフェイスの作成
- ファブリック設定の変更
- テンプレートの編集または作成

ただし、ネットワーク ステージャは次のアクションを実行できません。

- スイッチに設定を展開できません。
- SAN コントローラ Web UI または REST API から展開関連のアクションを実行できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。
- メンテナンス モードの切り替えはできません。
- 展開フリーズ モードでファブリックを移動したり、展開モードから解放したりすることはできません。
- パッチをインストールします。
- スイッチをアップグレードできません。
- ファブリックを作成または削除できません。
- スイッチをインポートまたは削除できません。

NDFC ネットワーク オペレータ

ネットワーク オペレータは、ファブリック ビルダー、ファブリック設定、構成のプレビュー、ポリシー、およびテンプレートを表示できます。ただし、ネットワーク オペレータは次の操作を実行できません。

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

ネットワーク オペレータとネットワーク ステージャの違いは、ネットワーク ステージャとして、既存のファブリックのインテントのみを定義できますが、それらの設定を展開できないことです。

ネットワーク ステージャロールを持つユーザがステージングした変更および編集を展開できるのは、ネットワーク管理者だけです。

デフォルトの認証ドメインの選択

Nexus ダッシュボードのデフォルトのログイン画面では、認証用のローカルドメインが選択されます。ドロップダウンリストから利用可能なドメインを選択することで、ログイン時にドメインを変更できます。

Nexus ダッシュボードは、ローカルおよびリモート認証をサポートしています。Nexus ダッシュボードのリモート認証プロバイダーには、RADIUS と TACACS が含まれます。認証サポートの詳細については、『Cisco Nexus ダッシュボード ユーザー ガイド、リリース 2.1.x』を参照してください。

次の表に、DCNM アクセスと NDFC アクセス間の RBAC の比較を示します。

DCNM 11.5(x)	NDFC 12.0.x および 12.1.x
• ユーザーのロールは 1 つです。 • すべての API とリソースは、この 1 つのロールでアクセスされます。	• ユーザーは、セキュリティドメインの Nexus ダッシュボードごとに異なるロールを持つことができます。 • セキュリティドメインには単一の Nexus ダッシュボードが含まれ、各 Nexus ダッシュボードには単一の NDFC ファブリックが含まれます。
DCNM のオプションへのアクセスを無効化または制限することにより、単一のロールがユーザーに関連付けられます。	単一のロールでは、選択したページに特権リソースのみが表示され、NDFC のその他のオプションでは、選択したリソースに関連付けられたセキュリティドメインに基づいて、制限されたアクセスがグレー表示されます。
シェル、ロール、およびオプションのアクセス制約を含む DCNM AV ペア形式。	シェル、ドメインを含む Nexus Dashboard AV Pair フォーマット。
展開タイプ LAN、SAN、または PMN に基づいてサポートされるロール。	network-admin、network-operator、device-upg-admin、network-stager、access-admin などのサポートされているロールは NDFC にあります。下位互換性のためのレガシー ロールのサポート。DCNM のネットワーク管理者としての Nexus ダッシュボード管理ロール。

次の表では、DCNM 11.5(x) AV ペアの形式について説明します。

Cisco DCNM Role	RADIUS Cisco-AV-Pair の値	TACACS+ シェル Cisco-AV-Pair ペアの値
network-operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"

次の表では、NDFC 12.x AV ペアの形式について説明します。

ユーザー ロール	AVPair 値
NDFC アクセス管理者	アクセス管理者
NDFC デバイス アップグレード管理者	Device-upg-admin
NDFC ネットワーク管理者	network-admin
NDFC ネットワーク オペレータ	network-operator
NDFC ネットワーク ステージャ	Network-stager

AV ペア文字列の形式は、特定のユーザーに対して読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかによって異なります。通常の文字列にはドメインが含まれており、その後にスラッシュ（/）で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ（|）で区切られています。

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

Nexus Dashboard のセキュリティ ドメイン

ユーザー ログインに関するアクセス制御情報には、ユーザー ID、パスワードなどの認証データが含まれます。認証データに基づいて、リソースに適宜アクセスできます。Cisco Nexus Dashboard の管理者は、セキュリティ ドメインを作成し、さまざまなリソース タイプ、リソース インスタンスをグループ化し、それらをセキュリティ ドメインにマッピングできます。管理者は各ユーザーの AV ペアを定義します。これにより、Cisco Nexus Dashboard のさまざまなリソースに対するユーザーのアクセス権限が定義されます。ファブリックを作成すると、Nexus ダッシュボードに同じファブリック名でサイトが作成されます。これらのサイトは、**Nexus Dashboard] > [サイト（Sites）]**で作成および表示できます。

SAN コントローラ REST API は、この情報を使用して、認可を確認することによってアクションを実行します。

> REST API にアクセスすると、渡されたペイロードを JSON 形式で確認できます。ペイロードが適切な JSON 形式であることを確認します。SAN コントローラリリース 11.x からアップグレードすると、各ファブリックは同じ名前の自動生成サイトにマッピングされます。これらすべてのサイトは、Nexus ダッシュボードの**すべて**のセキュリティ ドメインにマッピングされます。

すべてのリソースは、他のドメインに割り当てられたりマッピングされたりする前に、**すべて**のドメインに配置されます。すべてのセキュリティ ドメインには、Nexus ダッシュボードで使用可能なすべてのセキュリティ ドメインは含まれません。

AV ペア

セキュリティ ドメインのグループと各ドメインの読み取りおよび書き込みロールは、AV ペアを使用して指定されます。管理者は、各ユーザの AV ペアを定義します。AV ペアは、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限を定義します。

AV ペアの形式は次のとおりです。

```
"avpair": "shell:domains=security-domain/write-role-1|write-role-2,security-domain/write-role-1|write-role2/read-role-1|read-role-2"
```

例： `"avpair": "shell:domains=all/network-admin/app-user|network-operator"`

`all/admin/` はユーザーをスーパー ユーザーにします。そして`all/admin/` を使用する例は避けることをお勧めします。write ロールには read ロールも含まれます。したがって、`all/network-admin/` と `all/network-admin/network- admin` は同じです。

> SAN コントローラ リリース 12.0.1a から、SAN コントローラ リリース11.x で作成した既存の AV ペア フォーマットがサポートされます。ただし、新しい AV ペアを作成する場合は、上記の形式を使用します。shell:domains にスペースが含まれていないことを確認します。

AAA サーバー上での Cisco NX-OS のユーザー ロールおよび SNMPv3 パラメータの指定

AAA サーバー上で VSA cisco-AV-pair を使用して、次の形式で Cisco NX-OS デバイス
のユーザー ロールマッピングを指定できます：

```
shell:roles="roleA roleB ..."
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-AV-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュリティ ドメインの作成

Cisco Nexus Dashboard からセキュリティ ドメインを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. [管理（Administrative）] > **[セキュリティ（Security）]** の順に選択します。
3. **[セキュリティ ドメイン（Security Domain）]** タブに移動します。
4. **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。
5. 必要な詳細を入力し、**[作成（Create）]** をクリックします。

ユーザの作成

Cisco Nexus Dashboard からユーザを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. [管理（Administrative）] > **[ユーザー（Users）] の順に選択します。**
3. **[ローカル ユーザーの作成（Create Local User）]** をクリックします。
4. 必要な詳細を入力し、**[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。
5. ドロップダウン リストからドメインを選択します。
6. 適切なチェックボックスをオンにして、SAN コントローラ サービスの読み取りまたは書き込みロールを割り当てます。
7. **[保存（Save）]** をクリックします。

著作権