管理（Administration）

この章は次のトピックで構成されています。

DCNM サーバ

DCNM メニューには次のサブメニューが含まれます。

サービスの開始、再開、停止

デフォルトでは DCNM とそのスイッチ間の ICMP 接続は、パフォーマンス管理中に接続を検証します。ICMP を無効にすると、パフォーマンス管理データはスイッチから取得されません。このパラメータは、**サーバー プロパティ**で構成できます。Cisco DCNM Web UI から ICMP 接続チェックを無効にするには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、`skip.checkPingAndManageable` パラメータの値を `[true]` に設定します。

Performance Manager データベース（PM DB）の古いエントリをクリーンアップし、サービスを開始、再起動、または停止するには、Cisco DCNM Web UI から、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

サーバーの詳細を表示する **[ステータス（Status）]** ウィンドウが表示されます。

ステップ 2 **[アクション]** 列で、実行するアクションをクリックします。次の操作を実行できます。

- サービスを起動または再起動します。
- サービスを停止します。
- 古い PM DB エントリをクリーンアップします。
- Elasticsearch DB スキーマを再初期化します。

ステップ 3 **[ステータス（Status）]** 列でステータスを表示します。

What to do next

[ステータス（Status）] 列で最新のステータスを確認します。

Cisco DCNM リリース 11.4(1) から、次のサービスのステータスも表示できます。

Note 次のサービスは、OVA/ISO 展開でのみ利用できます。

Windows または Linux の展開には適用されません。

- NTPD サーバー：DCNM OVA で実行されている NTPD サービス、IP アドレス、およびサービスがバインドされているポート。
- DHCP サーバー：DCNM OVA で実行されている DHCP サービス、IP アドレス、およびサービスがバインドされているポート。
- SNMP トラップ
- syslogレシーバ

これらのサービスの DCNM サーバーは次のとおりです。

サービス名	DCNM サーバー
NTPD サーバー	0.0.0.0:123
DHCP サーバー	0.0.0.0:67
SNMP トラップ	0.0.0.0:2162
[Syslogサーバ（Syslog Server）]	0.0.0.0:514

コマンド テーブルの使用

コマンド テーブルには、サーバー ステータスとサーバー管理ユーティリティ スクリプトに関する情報を提供する新しいダイアログボックスを起動するコマンドへのリンクが含まれています。これらのコマンドは、サーバー CLI で直接実行できます。

- **ifconfig**：このリンクをクリックして、Cisco DCNM サーバで使用されるインターフェイス パラメータ、IP アドレス、およびネットマスクに関する情報を表示します。
- **appmgr status all**：このリンクをクリックして、現在実行されているさまざまなサービスのステータスをチェックする DCNM サーバー管理ユーティリティ スクリプトを表示します。
- **appmgr show vmware-info**：このリンクをクリックして、仮想マシンの CPU とメモリに関する情報を表示します。
- **時計**：このリンクをクリックして、時間、ゾーン情報などのサーバー クロックの詳細に関する情報を表示します。

Note コマンド セクションは、OVA または ISO のインストールにのみ適用されます。

[カスタマイズ（Customization）]

Cisco DCNM リリース 11.3(1) 以降、Web UI ログイン ページで背景画像とメッセージを変更できます。この機能は、同時に多数のインスタンスを実行している場合に、DCNM インスタンスを区別するのに役立ちます。ログイン ページで企業ブランドの背景を使用することもできます。[デフォルトに戻す（Restore Defaults）] をクリックして、カスタマイズを元のデフォルト値にリセットします。

カスタムを削除してデフォルト値に復元するには、**[デフォルトの復元（Restore defaults）]** をクリックします。

ログイン画像

この機能では、 Cisco DCNM Web UI のログイン ページの背景画像を変更できます。DCNM のインスタンスが多数ある場合、これは、背景画像に基づいて正しい DCNM インスタンスを識別するのに役立ちます。

Cisco DCNM Web UI ログイン ページのデフォルトの背景画像を編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [カスタマイズ（DCNM Server）]** を選択します。
2. ログイン画像領域で、**[追加（+）（Add (+)）]** アイコンをクリックします。

   ローカル ディレクトリからアップロードする必要がある画像を参照します。背景画像には、JPEG、GIF、PNG、IVL、および SVG のファイル形式を使用できます。
3. 画像を選択し、**[開く（Open）]** をクリックします。

   ステータス メッセージが右下隅に表示されます。

ログイン画像アップロード成功

（注） 読み込み時間を短縮するには、拡大縮小された画像をアップロードすることをお勧めします。

アップロードされた画像が選択され、背景画像として適用されます。

4. 既存の画像をログイン画像として選択するには、画像を選択し、右下隅にメッセージが表示されるまで待ちます。
5. デフォルトのログイン画像に戻すには、**[デフォルトに戻す（Restore Defaults）]**をクリックします。

本日のメッセージ（MOTD）

この機能を使用すると、Cisco DCNM Web UI ログイン ページにメッセージを追加できます。構成された頻度でローテーションするメッセージのリストを表示できます。この機能を使用すると、ログイン ページで重要なメッセージをユーザーに伝えることができます。

Cisco DCNM Web UI ログイン ページでその日のメッセージを追加または編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバー] > [カスタマイズ（Customization）]** を選択します。
2. **[本日のメッセージ（MOTD）]**フィールドに、ログインページに表示する必要があるメッセージを入力します。
3. [保存（Save）] をクリックします。

ログ情報の表示

Performance Manager、SAN 管理サーバ、SME サーバ、Web レポート、Web サーバ、および Web サービスのログを表示できます。しかし、これらのプロセスには、ログ ファイルの情報を表示できる GUI はありません。エラーを調べる場合は、表示できるようにこれらのファイルを保存してください。

Note フェデレーション内のリモート サーバからログを表示することはできません。

Cisco DCNM Web UI からログを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [ログ（Logs）]** を選択します。

左列にログのツリーベース リストが表示されます。ツリーの下には、フェデレーション内のすべてのサーバのノードがあります。ログ ファイルは、対応するサーバ ノードの下にあります。

ステップ 2 ツリーの各ノードの下にあるログ ファイルをクリックして、右側に表示します。

ステップ 3 各サーバのツリー ノードをダブルクリックして、そのサーバからログ ファイルを含むZIP ファイルをダウンロードします。

ステップ 4 (Optional) **[テクニカル サポートの生成（Generate Techsupport）]** をクリックして、テクニカル サポートに必要なファイルを生成およびダウンロードします。

このファイルには、ログ ファイルに加えて詳細情報が含まれています。

Note OVA および ISO の展開では TAR.GZ ファイルがダウンロードされ、他のすべての展開では ZIP ファイルがダウンロードされます。 CLI で **appmgr tech_support** コマンドを使用して、techsupport ファイルを生成できます。

ステップ 5 (Optional) ログを印刷するには、右上隅の **[印刷（Print）]** アイコンをクリックします。

サーバ プロパティ

DCNM サーバでデフォルト値として入力されるパラメータを設定できます。

Cisco DCNM Web UI から DCNM サーバのパラメータを設定するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

ステップ 2 **[変更を適用（Apply Changes）]** をクリックしてサーバ設定を保存します。

SFTP/SCP ログイン情報の構成

デバイス構成を収集し、構成をデバイスに復元するには、ファイル サーバーが必要です。

Cisco DCNM Web UI からファイル ストアの SFTP/SCP ログイン情報を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理] > [DCNM サーバー] > [FTP クレデンシャルのアーカイブ]** を選択します。

「**FTP ログイン情報のアーカイブ**」ウィンドウが表示されます。

Note ログイン情報は、新しい OVA および ISO インストール用に自動入力されます。

ステップ 2 **[サーバー タイプ]** フィールドで、ラジオ ボタンを使用して **SFTP** を選択します。

Note
- バックアップ操作を実行するには、SFTP サーバーが必要です。SFTP サーバーは外部サーバーにすることができます。SFTP ディレクトリは Linux/SSH の絶対パス形式である必要があり、SFTP ユーザーへの読み取り/書き込みアクセスが必要です。
- 外部サーバーを使用している場合は、**[管理] > [DCNM サーバ] > [サーバー プロパティ]** の **server.FileServerAddress** フィールドにその IP アドレスを入力します。
- **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **nat.enabled** フィールドが true の場合は、**server.FileServerAddress** フィールドに NAT デバイスの IP を入力する必要があり、SFTP サーバはローカルである必要があります。

a) [ユーザー名（User Name）] と [パスワード（Password）] に入力します。

Note リリース 11.3(1) 以降、OVA/ISO インストールの場合、**sysadmin** ユーザー ログイン情報を使用してルート ディレクトリにアクセスします。

b) **ディレクトリ** パスを入力します。

パスは Linux の絶対パス形式である必要があります。

デバイスで SFTP が使用できない場合は、ミニ SFTP、Solarwinds などのサードパーティの SFTP アプリケーションを使用できます。外部 SFTP を使用する場合は、STFP ディレクトリ パスに相対パスを指定する必要があります。たとえば、この手順の最後にあるユースケースを検討してください。

Note リリース 11.3(1) 以降、OVA/ISO インストールの場合、ディレクトリを `/home/sysadmin` として入力します。

c) **[検証スイッチ（Verification Switch）]** ドロップダウン リストから、スイッチを選択します。

d) **[適用（Apply）]** をクリックして、資格情報を保存します。

e) **[確認して適用]** をクリックして、SFTP とスイッチに接続があるかどうかを確認し、構成を保存します。

検証中にエラーが発生した場合、新しい変更は保存されません。

f) **[Clear SSH Hosts]** をクリックして、すべてのスイッチまたは選択したスイッチの SSH ホストをクリアします。

いずれかのスイッチで障害が発生すると、エラー メッセージが表示されます。**[構成] > [バックアップ] > [スイッチ構成] > [アーカイブ ジョブ] > [ジョブ実行の詳細]** に移動して、成功したスイッチと失敗したスイッチの数を表示します。

ステップ 3 **[サーバー タイプ（Server Type）]** フィールドで、ラジオ ボタンを使用して **TFTP** を選択します。

Cisco DCNM は、データ転送にローカル TFTP サーバーを使用します。DCNM サーバーで実行されている外部 TFTP サーバーがないことを確認します。

Note ユーザー切り替えの役割に copy コマンドが含まれていることを確認してください。オペレーターの役割は、許可拒否（*permission denied*）エラーを受け取ります。**[検出]** ウィンドウでログイン情報を変更できます。**[インベントリ（Inventory）] > [検出（Discovery）]** に移動します。

a) **[検証スイッチ（Verification Switch）]** ドロップダウン リストから、スイッチを選択します。
b) **[適用]** をクリックして、ログイン情報をすべての場所に保存します。
c) **[確認 & 適用]** をクリックして、TFTP とスイッチに接続があるかどうかを確認し、設定を保存します。

検証中にエラーが発生した場合、新しい変更は保存されません。

ステップ 4 **[サーバ タイプ（Server Type）]** フィールドで、ラジオ ボタンを使用して **[SCP]** を選択します。

Note
- バックアップ操作を実行するには、SCP サーバーが必要です。SCP サーバーは外部サーバーにすることができます。SCP ディレクトリは Linux/SSH の絶対パス形式である必要があり、SCP ユーザーへの読み取り/書き込みアクセスが必要です。
- 外部サーバーを使用している場合は、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **server.FileServerAddress** フィールドにその IP アドレスを入力します。
- **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の **[nat.enabled]** フィールドが true の場合は、**server.FileServerAddress** フィールドに NAT デバイスの IP を入力する必要があり、サーバーはローカルである必要があります。

a) [ユーザー名（User Name）] と [パスワード（Password）] に入力します。
b) **ディレクトリ** パスを入力します。

パスは Linux の絶対パス形式である必要があります。

デバイスで SCP を使用できない場合は、mini-SCP、Solarwinds などの外部 SCP アプリケーションを使用します。外部 SCP を使用する場合は、SCP ディレクトリ パスに相対パスを指定する必要があります。たとえば、この手順の最後にあるユース ケースを検討してください。

c) **[検証スイッチ（Verification Switches）]** ドロップダウンから、スイッチを選択します。
d) **[適用]** をクリックして、ログイン情報をすべての場所に保存します。

e) **[確認して適用（Verify & Apply）]** をクリックして、SCP とスイッチに接続があるかどうかを確認し、構成を保存します。検証中にエラーが発生した場合、新しい変更は保存されません。

f) **[Clear SSH Hosts]** をクリックして、すべてのスイッチまたは選択したスイッチの SSH ホストをクリアします。

いずれかのスイッチに障害があると、エラー メッセージが表示されます。成功したスイッチと失敗したスイッチの数を表示するには、**[構成（Configure）] > [バックアップ（Backup）] > [スイッチの構成（Switch Configuration）] > [アーカイブ ジョブ（Archive Jobs）] > [ジョブ実行の詳細（Job Execution Details）]** に移動します。

ステップ 5 **[構成（Configuration）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Templates Library）] > [ジョブ（Jobs）]** を選択して、個々のデバイスの検証ステータスを表示します。

バックアップされた構成はファイル サーバから削除され、ファイル システムに保存されます。

SFTP ディレクトリ パス

事例 1

Cisco DCNM が OVA、ISO、または Linux などの Linux プラットフォームにインストールされており、テスト フォルダが `/test/sftp/` にある場合は、SFTP ディレクトリの完全なパスを指定する必要があります。[SFTP ディレクトリ（SFTP Directory）] フィールドで、`/test/sftp` と入力します。

使用例 2：

Cisco DCNM が Windows プラットフォームにインストールされていて、テスト フォルダが `C://Users/test/sftp/` にある場合は、SFTP ディレクトリの相対パスを指定する必要があります。[SFTP ディレクトリ（SFTP Directory）] フィールドで、`/` と入力します。

次に例を示します。

- 外部 SFTP のパスが `C://Users/test/sftp/` の場合、Cisco DCNM SFTP ディレクトリ パスは `/` である必要があります。
- 外部 SFTP のパスが `C://Users/test` の場合、Cisco DCNM SFTP ディレクトリのパスは `/sftp/` である必要があります。

SCP ディレクトリ パスの例

事例 1

Cisco DCNM が OVA、ISO、または Linux などの Linux プラットフォームにインストールされていて、テスト フォルダが /test/scp/ にある場合は、SCP ディレクトリの完全なパスを指定する必要があります。**[SCP ディレクトリ（SCP Directory）]** フィールドで、`/test/scp` と入力します。

事例 2

Cisco DCNM が Windows プラットフォームにインストールされていて、テスト フォルダが C://Users/test/scp/ にある場合は、SCP ディレクトリの相対パスを指定する必要があります。**[SCP ディレクトリ（SCP Directory）]** フィールドで、/ と入力します。

次に例を示します。

- 外部 SCP のパスが C://Users/test/scp/ の場合、Cisco DCNM SCP ディレクトリ パスは / である必要があります。
- 外部 SCP のパスが C://Users/test の場合、Cisco DCNM SCP ディレクトリ パスは /scp/ である必要があります。

モジュラ デバイスのサポート

大きな変更をあまり必要としない新しいハードウェアをサポートするために、次の DCNM リリースを待たずにパッチを配布できます。**[モジュラ デバイス サポート（Modular Device Support）]**は、DCNM パッチ リリースの配布と適用に役立ちます。認証された DCNM 管理者は、パッチを本番環境のセットアップに適用できます。パッチ リリースは、次のシナリオに適用されます。

- シャーシやライン カードなどの新しいハードウェアをサポート
- 最新の NX-OS バージョンをサポート
- 重要な修正をパッチとしてサポート

Cisco DCNM Web UI からパッチの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [モジュラ デバイス サポート（Modular Device Support）]** を選択します。

ウィンドウの左側に **[DCNM サーバ（DCNM Servers）]** 列が表示され、右側に **[文殊ら デバイス サポート上布（Modular Device support information）]** ウィンドウが表示されます。

ステップ 2 **[DCNM サーバ（DCNM Servers）]**を展開して、すべての DCNM サーバを表示します。

これには、**[モジュラ デバイス サポート情報（Modular Device support information）]** テーブルのバージョン番号、対応するプラットフォーム、サポートされるシャーシ、サポートされる NX-OS バージョン、PID サポート、バックアップ ディレクトリ、および最後のパッチ展開時間とともに、インストールされたパッチのリストが含まれます。

What to do next

パッチを適用してロールバックする方法の詳細については、http://www.cisco.com/go/dcnm を参照してください。

スイッチ グループの管理

Cisco DCNM Web UI を使用して、スイッチ グループを構成できます。スイッチをグループに追加、削除、または移動したり、スイッチをグループから別のグループに移動したりできます。

この項の内容は、次のとおりです。

スイッチ グループの追加

Cisco DCNM Web UI からスイッチ グループを追加するために次の手順を実行します。

Procedure

ステップ 1 **[管理] > [DCNM サーバー] > [スイッチ グループ]** を選択します。

ステップ 2 [追加（Add）] アイコンをクリックします。

[グループを追加（Add Groups）] ウィンドウが表示され、スイッチ グループの名前を入力できます。

ステップ 3 スイッチ グループの名前を入力し、**[追加（Add）]** をクリックしてスイッチ グループの追加を完了します。

スイッチ グループ名の検証、および最大のツリーの深さは 10 です。新しいスイッチ グループを追加する前に親グループを選択しなかった場合、新しいグループは階層の最上位に追加されます。

グループまたはグループのメンバーの削除

Cisco DCNM Web UI から、グループまたはグループのメンバーを削除できます。グループを削除すると、関連するグループも削除されます。削除されたグループのファブリックまたはイーサネット スイッチは、デフォルトの SAN またはローカル エリア ネットワーク（LAN）に移動されます。

グループまたはグループのメンバーを Cisco DCNM Web UI から削除するには、次の手順を実行します。

Procedure

ステップ 1 削除するスイッチ グループまたはグループのメンバーを選択します。

ステップ 2 **[削除（Remove）]** アイコンをクリックします。

スイッチ グループまたはグループのメンバーの削除を確認するダイアログ ボックスがプロンプトします。

ステップ 3 **[はい（Yes）]** をクリックして削除するか、**[いいえ（No）]** をクリックしてアクションをキャンセルします。

スイッチ グループを別のグループに移動する

Cisco DCNM Web UI からスイッチ グループを別のグループに移動するには、次の手順を実行します。

Procedure

ステップ 1 スイッチまたはスイッチ グループを選択します。

ステップ 2 強調表示されたスイッチまたはスイッチ グループを別のグループにドラッグします。

複数のスイッチを異なるスイッチ グループ間で移動するには、**Ctrl** キーまたは **Shift** キーを使用します。

スイッチまたはスイッチ グループが表示されます。現在、ユーザーは、新しいグループの下のグループ レベルで複数のスイッチを移動することはできません。

Note グループ レベルで複数のスイッチを移動することはできません。グループとスイッチを混在させることはできません。

カスタム ポート グループの管理

カスタム ポート グループは、グループ内のインターフェイスのパフォーマンスをテストするのに役立ちます。定義されたカスタム ポートとその構成を表示できます。

このセクションは、次のトピックで構成されています。

カスタム ポート グループを追加

Cisco DCNM Web UI からカスタム ポート グループを追加するために、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

[カスタム ポート グループ（Custom Port Groups）] ウィンドウが表示されます。

ステップ 2 **[ユーザー定義グループ（User-Defined Groups）]** ブロックで、**[追加（Add）]** アイコンをクリックします。

ステップ 3 **[グループの追加ダイアログ（Add Group Dialog）]** ウィンドウで、カスタム ポート グループの名前を入力します。

ステップ 4 [追加] をクリックします。

[ユーザー定義グループ（User-Defined Groups）] 領域にカスタム ポート グループが作成されます。

スイッチおよびインターフェイスをポート グループに構成する

Cisco DCNM Web UI からのスイッチとインターフェイスを含めるようにカスタム ポート グループを構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ（User-Defined Groups）]** エリアで、スイッチとインターフェイスを追加するポート グループを選択します。

ステップ 3 **[構成（Configurations）]** エリアで、**[メンバーの追加（Add Member）]** をクリックします。

選択したカスタム ポート グループの **[ポート構成（Port Configuration）]** ウィンドウが表示されます。

ステップ 4 **[スイッチ（Switches）]** タブで、カスタム ポート グループに含めるスイッチを選択します。

使用可能な**[インターフェイス（Interfaces）]**のリストが表示されます。

ステップ 5 すべてのインターフェイスを選択して、パフォーマンスを確認します。

ステップ 6 [送信（Submit）] をクリックします。

インターフェイスのリストがカスタム ポート グループに追加されます。

ポート グループ メンバーを削除

カスタム ポート グループのポート グループ メンバーを Cisco DCNM Web UI から削除または削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 > DCNM サーバ > カスタム ポート グループ（Administration > DCNM Server > Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ]** エリアで、ポート グループを選択します。

ステップ 3 **[構成（Configuration）]** エリアで、削除する必要があるスイッチ名とインターフェイスを選択します。

ステップ 4 **[ユーザー定義グループ（User Defined Groups）]** エリアで、メンバーを削除する必要があるグループを選択します。

ステップ 5 **[メンバーを削除（Remove Member）]** をクリックします。

確認ウィンドウが表示されます。

ステップ 6 **[はい（Yes）]** をクリックして、カスタム ポート グループからメンバーを削除します。

ポート グループの削除

Cisco DCNM ウェブ UI からポート グループを除去または削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [カスタム ポート グループ（Custom Port Groups）]** を選択します。

ステップ 2 **[ユーザー定義グループ（User Defined Groups）]** エリアで、削除する必要があるグループを選択します。

ステップ 3 **[削除（Remove）]** をクリックします。

確認ウィンドウが表示されます。

ステップ 4 **[はい（Yes）]** をクリックして、カスタム グループを削除します。

サーバー フェデレーションの表示

Note フェイルオーバーが正しく機能するためには、フェデレーション セットアップに少なくとも 3 つのノードが必要です。2 ノードのフェデレーション設定では、サーバーの 1 つがダウンしている場合、Elasticsearch はクラスタを形成できないため、Web UI は一貫性のない動作をする可能性があります。3 ノードのフェデレーション設定の場合、2 つのサーバーがダウンすると、WebUI の一貫性のない動作が見られます。

Note フェデレーションのスイッチオーバーまたはフェイルオーバーの後は、毎回ブラウザのキャッシュと Cookie をクリアするようにしてください。

Cisco DCNM でフェデレーション サーバー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 **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** を選択します。

サーバーのリストとその IP アドレス、ステータス、場所、現地時間、およびデータ ソースが表示されます。

ステップ 2 **[自動フェールオーバーを有効にする（Enable Automatic Failover）]** チェック ボックスを使用して、フェールオーバー機能をオンまたはオフにします。

ステップ 3 **[場所（Location）]** 列で、ダブルクリックして場所を編集します。

フェデレーション内のいずれかのサーバーのステータスが**非アクティブ**の場合、サーバーのステータスが**アクティブ**に変更されない限り、一部の機能が動作しないことがあります。

Note Cisco DCNM をアップグレードする前に、**[自動フェールオーバーを有効にする（Enable Automatic Failover）]** がオフになっていることを確認してください。そうしないと、フェデレーション内の 1 つのサーバーがダウンすると、デバイスは、アップグレード後に最初に起動する別の DCNM サーバーに移動されます。DCNM アップグレードの自動移動を防止するには、フェデレーション内のすべての DCNM で自動移動を無効にして、DCNM サーバーを 1 つずつアップグレードする必要があります。すべての DCNM が正常にアップグレードされ、通常通り実行された後にのみ、自動移動を再度有効にします。

Note DCNM フェデレーションでは、**[自動フェールオーバーを有効にする]** が有効になっている場合、DCNM がダウンすると、その管理下にあるデバイスが他の DCNM に移動されます。ただし、DCNM が戻った後、デバイスは元に戻りません。

Note Cisco DCNM Federation をアップグレードするときは、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** ページに再度アクセスし、アップグレードの完了後に Elasticsearch cluster sync コマンドを実行する必要があります。これにより、Elasticsearch 構成が更新され、パフォーマンスのモニタリングが再開されます。Elasticsearch cluster sync コマンドを実行するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [フェデレーション（Federation）]** ページで [Elasticsearch クラスタリング（Elasticsearch clustering）] ボタンを有効にする必要があります。パフォーマンス モニタリングを再開するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー ステータス（Server Status）]** を選択し、緑色のボタンをクリックします。

ElasticSearch Cluster セクションには、エラスティック検索に関する詳細が表示されます。次のフィールドがあります。

フィールド	説明
名前	エラスティック検索クラスタの名前を指定します。

フィールド	説明
ノード	クラスタ化されたインスタンスの数を指定します。
ステータス（Status）	クラスタが有効かどうかを指定します。クラスタが有効になっていない場合、ステータスは黄色です。クラスタが有効になっている場合、ステータスは緑です。

Elasticsearch クラスタリング

Note **ElasticSearch Clustering** sync-up オプションは、フェデレーション設定のプライマリ ノードでのみ使用できます。

フェデレーション サーバーに関連付けられている各エラスティック検索ノードを Elasticsearch クラスタリングに同期するには、次の手順を実行します。

Procedure

ステップ 1 **[フェデレーション（Federation）]** ウィンドウで、**[Elasticsearch クラスタリング（ElasticSearch Clustering）]** をクリックします。**[Elastic Search クラスタリング（Elastic Search Clustering）]** ポップアップ ウィンドウが表示されます。

ステップ 2 **[適用 (Apply)]** をクリックします。
この操作により、フェデレーションサーバーに関連付けられている各エラスティック検索ノードがエラスティック検索クラスタに同期されます。この操作は、エラスティック検索をデータストアとして使用するすべての機能に悪影響を及ぼします。一部の機能は、エラスティック検索サービスの再開後に進行中のデータ同期操作の影響を受けます。

マルチ サイト マネージャ

Procedure

ステップ 1 Multi-Site-Manager（MsM）は、DCNM によってグローバルに管理されているスイッチをユーザーが検索するための単一のペインを提供します。MSM はリアルタイム検索を実行して、IP アドレス、名前、または MAC アドレスに基づいて特定の仮想マシンのトラフィックをグローバルに処理し、セグメント ID に基づいて VXLAN をサポートするスイッチを見つけることができます。スイッチのみを起動するためのハイパーリンクを提供します。このウィンドウは、

リモートサイト登録の役割も果たします。登録により、現在のDCNMサーバがリモートDCNMサーバまたはサイトにアクセスできるようになります。リモート サイトが現在の DCNM サーバにアクセスするには、リモート サイトでも登録が必要です。

ステップ 2 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。

MsMウィンドウには、リモートサイトの全体的な健全性またはステータス、およびアプリケーションの健全性が表示されます。

ステップ 3 **[スイッチ、VM IP、VM 名、MAC（Switch, VM IP, VM Name, MAC）]、[セグメント ID（Segment ID）]** で検索できます。

ステップ 4 **[+ DCNM サーバの追加（+Add DCNM Server）]** をクリックして、新しい DCNM サーバを追加できます。**[リモート DCNM サーバ情報の入力（Enter Remote DCNM Server Information）]** ウィンドウが開きます。必要な情報を入力し、**[OK]** をクリックして保存します。

ステップ 5 **[すべてのサイトの更新（Refresh All Sites）]** をクリックし、更新された情報を表示します。

ライセンスの管理

[ライセンス付与の管理 (Manage Licensing)] メニューには、次のサブメニューがあります。

ライセンスの管理

[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] を選択すると、既存のCisco DCNMライセンスを表示できます。次のタブでライセンスを表示して割り当てることができます。

- **ライセンスの割り当て**
- **スマート ライセンス**
- **サーバ ライセンス ファイル**

Note デフォルトでは、**[ライセンスの割り当て（License Assignments）]** タブが表示されます。

次の表に、SAN および LAN のライセンス情報を示します。

フィールド	説明
License	SAN または LAN を指定します。

フィールド	説明
無料/合計サーバベースのライセンス	ライセンスの総数のうち、購入する無料ライセンスの数を指定します。新規インストールのライセンスの総数は 50 です。ただし、インライン アップグレードの場合、ライセンスの合計数は 500 のままになります。
ライセンスなし/合計（スイッチ/VDC）	スイッチまたはVDC の総数のうち、ライセンスのないスイッチまたは VDC の数を指定します。
購入する必要があります	購入するライセンス数を指定します。

このセクションは、次のトピックで構成されています。

ライセンスの割り当て

次の表に、すべてのスイッチまたは VDC のライセンス割り当ての詳細を示します。

フィールド	説明
グループ	グループがファブリックか LAN かを表示します。
スイッチ名	スイッチの名前が示されます。
WWN/シャーシ ID	World Wide Name またはシャーシ ID を表示します。
モデル	デバイスのモデルが示されます。DS-C9124 や N5K-C5020P-BF など。
ライセンスの状態	次のいずれかの、スイッチのライセンス ステータスが示されます。 • 永続 • 評価用 • Unlicensed • N/A • 期限切れ • 無効 • スマート

フィールド	説明
License Type	次のいずれかの、スイッチのライセンス ステータスが示されます。 • DCNM サーバー • スイッチ • スマート • オナー • スイッチスマート
期限日 （Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** 列の下のテキストは、7日で期限切れになるライセンスの場合は赤で表示されます。
ライセンスの割り当て	行を選択し、ツールバーのこのオプションをクリックしてライセンスを割り当てます。
割り当ての解除	ライセンスの割り当てを解除するには、行を選択し、ツールバーのこのオプションをクリックします。 **Note** ファブリック内のすべてのスイッチのライセンスの割り当てを解除すると、ファブリックもライセンスがなくなります。ただし、ファブリックのライセンスの割り当てを解除した後、フェデレーション セットアップで PM サービスを再起動して、ファブリックが **[SAN収集（SAN Collection）]** ウィンドウに表示されないようにします。ファブリックを 1 つのノードから別のノードに正常に移動するには、PM を再起動する必要があります。
すべて割り当て	ツールバーのこのオプションをクリックしてテーブルを更新し、テーブル内のすべてのアイテムにライセンスを割り当てます。
すべて割り当て解除	ツールバーのこのオプションをクリックしてテーブルを更新し、すべてのライセンスの割り当てを解除します。

Note ライセンスの割り当てまたは割り当て解除を行うには、ネットワーク管理者権限が必要です。

ファブリックが最初に検出されたときに、スイッチに有効なスイッチベースのライセンスがない場合、ライセンスはファイルライセンスプールからファブリックに自動的に割り当てられ、プール内にライセンスが残っていない状態になります。既存のファブリックがあり新しいス

イッチがファブリックに追加されたとき、ファイル ライセンス プールで使用可能なライセンスがあり、まだスイッチベースのライセンスがない場合は、新しいスイッチにライセンスが割り当てられます。

スマート ライセンスを登録した後、永久ライセンスを持たないスイッチの **[ライセンスの割り当て（Assign License）]** をクリックすると、スマート ライセンスがスイッチに割り当てられます。割り当てられるライセンスの優先順位は、次の順序です。

1. **永続**
2. **スマート**
3. **評価用**

POAP を介してスイッチにライセンスを割り当てるには、『DCNM ライセンス ガイド』を参照してください。

スマート ライセンスを無効にすると、スマート ライセンスされたスイッチのライセンスの割り当てが解除されます。

評価ライセンスは、スマートライセンスをサポートしていないスイッチに割り当てられます。ライセンス状態は **Eval** で、ライセンス タイプは **DCNM-Server** です。スマート ライセンスをサポートするスイッチのリストを表示するには、『*Cisco DCNM* ライセンス ガイド、リリース *11.x*』を参照してください。

スマート ライセンス

Cisco DCNM リリース 11.1（1）からスマート ライセンシング機能を使用して、デバイス レベルでライセンスを管理し、必要に応じて更新します。Cisco DCNM Web UI から、**管理（Smart License Administration）] > [ライセンス管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。Cisco スマート ライセンスの簡単な紹介、メニューバー、および**[スイッチ ライセンス（Switch Licenses）]**エリアが表示されます。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマート ライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェア ライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（https://software.cisco.com/software/csws/ws/platform/home）。

シスコライセンスの詳細な概要については、https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html を参照してください。

概要で、**[ここをクリック（Click Here）]** をクリックして、スマート ソフトウェア ライセンスに関する情報を表示します。

メニューバーには次のアイコンがあります。

- **[登録状況（Registration Status）]**：クリックするとポップアップ ウィンドウに現在の登録の詳細が表示されます。スマート ライセンシングが有効になっていない場合、値は **UNCONFIGURED** です。登録せずにスマート ライセンシングを有効にすると、値は **DEREGISTERED** に設定されます。登録後、値は **REGISTERED** に設定されます。登録ステータスをクリックして、最後のアクション、アカウントの詳細、およびその他の登録の詳細を **[登録の詳細（Registration Details）]** ポップアップ ウィンドウに表示します。
- **[ライセンスのステータス（License Status）]**:ライセンスのステータスを指定しますスマート ライセンシングが有効になっていない場合、値は **UNCONFIGURED** です。登録せずにスマート ライセンシングを有効にすると、値は **NO LICENSES IN USE** に設定されます。値は、ライセンスを登録して割り当てると、**AUTHORIZED** または **OUT-OF-COMPLIANCE** に設定されます。**[ライセンス認証の詳細（License Authorization Details）]** ポップアップ ウィンドウで、最後のアクション、最後の認証試行、次の認証試行、および認証の有効期限を表示するには、ライセンス ステータスをクリックします。
- **[コントロール（Control）]**：スマート ライセンスの有効化または無効化、トークンの登録、認証の更新を行うことができます。

次の表で、「**スイッチ ライセンス**」の項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
名前	ライセンス名を指定します。
数	使用するライセンスの数を指定します。
ステータス	使用されているライセンスのステータスを指定します。有効な値は、**[認証済み（Authorized）]** と **[コンプライアンス違反（Out of Compliance）]** です。
説明	ライセンスのタイプと詳細を指定します。
最終更新	スイッチ ライセンスが最後に更新されたときのタイムスタンプを指定します。
プリント	スイッチ ライセンスの詳細を印刷できます。
エクスポート	ライセンスの詳細をエクスポートできます。

Cisco Smart Software Manager でアカウントから製品ライセンスを削除した後、スマート ライセンスを無効にして、再度登録します。

スマート ライセンスの有効化

Cisco DCNM Web UI からスマート ライセンスを有効にするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[コントロール（Control）]** をクリックし、ドロップダウン リストで **[イネーブル化（Enable）]** を選択して、スマート ライセンスを有効にします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックします。

DCNM インスタンスを登録する手順が表示されます。

登録ステータスが **UNCONFIGURED** から **DEREGISTERED** に変わり、ライセンス ステータスが **UNCONFIGURED** から **[使用されているライセンスはありません（No Licenses in Use）]** に変わります。

Cisco DCNM インスタンスの登録

Before you begin

Cisco Smart Software Manager のトークンを作成します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[登録（Register）]** を選択します。

[登録（Register）] ウィンドウが表示されます。

ステップ 3 スマート ライセンス エージェントを登録するには、[トランスポート（Transport）] オプションを選択します。

次のオプションがあります。

- **デフォルト：NDFC はシスコのライセンシング サーバと直接通信します**

  このオプションは、次の URL を使用します。
  https://tools.cisco.com/its/service/oddce/services/DDCEService

- **トランスポート ゲートウェイ（Transport Gateway） - ゲートウェイまたはサテライト経由のプロキシ**

  このオプションを選択する場合は、URL を入力します。

- **プロキシ**：**中間 HTTP または HTTPS プロキシ経由のプロキシ**

  このオプションを選択する場合は、URL とポートを入力します。

ステップ 4 **[トークン（Token）]** フィールドに登録トークンを入力します。

ステップ 5 ライセンスを登録するために、**[送信（Submit）]** をクリックします。

登録ステータスが **[登録抹消（DEREGISTERED）]** から **[登録済み（REGISTERED）]** に変わります。スイッチ ライセンスの名前、数、およびステータスが表示されます。

[登録ステータス：**登録済み（Registration Status: REGISTERED）]** をクリックして、登録されたトークンの詳細を表示します。

スイッチの詳細は、**[ライセンス割り当て（License Assignments）]** タブの **[スイッチ/VDC（Switches/VDCs）]** セクションで更新されます。スマート ライセンス オプションを使用してライセンスが付与されたスイッチのライセンス タイプとライセンス状態は **Smart** です。

What to do next

登録後に発生した通信エラーのトラブルシューティングを行います。

通信エラーのトラブルシューティング

登録中の通信エラーを解決するには、次の手順を実行します。

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 次のパスからサーバー プロパティ ファイルを開きます：/usr/local/cisco/dcm/fm/conf/server.properties

Note Windows のサーバー プロパティ ファイルは、次の場所にあります：C:/Program Files/Cisco/dcm/fm/conf/server.properties

ステップ 3 サーバー プロパティ ファイルに次のプロパティを含めます：

```
#cisco.smart.license.production=false #smartlicense.url.transport=https://
CiscoSatellite_Server_IP /Transportgateway/services/DeviceRequestHandler
```

ステップ 4 次のシンタックスで、/etc/hosts ファイルのホスト データベースにある Cisco サテライトの詳細を更新します：*Satellite_Server_IP* CiscoSatellite

ステップ 5 DCNM サービスを開始します。

認証を更新

登録済みの場合にのみ、承認を手動で更新できます。自動再承認は定期的に行われます。**[ライセンス ステータス（License Status）]** をクリックして、次回の自動再承認に関する詳細を表示します。Cisco DCNM Web UI から承認を更新するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[承認の更新（Renew Authorization）]** を選択して、ライセンス承認を更新します。

更新がある場合は、更新を取得する要求が Cisco Smart Software Manager に送信されます。更新後、**[スマート ライセンス（Smart Licenses）]** ウィンドウが更新されます。

スマート ソフトウェア ライセンスの無効化

Cisco DCNM Web UI からスマート ライセンスを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** を選択し、**[無効化（Disable）]** を選択して、スマート ライセンスを無効にします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックします。

このトークンを使用するスイッチのライセンス ステータスは、**[ライセンスの割り当て（License Assignments）]** タブで、**[ライセンスなし（Unlicensed）]** に変わります。このトークンは、Cisco Smart Software Manager の **[製品インスタンス（Product Instances）]** タブの下のリストから削除されます。

スマート ライセンスが利用できず、スマート ライセンスを無効にした場合は、**[ライセンスの割り当て（License Assignments）]** タブからライセンスを手動で解放します。

スイッチ スマート ライセンス

スマート ライセンスでスイッチが事前構成されている場合、DCNM がスイッチ スマート ライセンスを検証し割り当てます。Cisco DCNM UI を使用してスイッチにライセンスを割り当てる

には、**[管理（Administration）]>[ライセンスの管理（Manage Licensing）]>[ライセンスの割り当て（Assign License）]** または **[すべて割り当て（Assign All）]** を選択します。

（注） Cisco NX-OS リリース 9.3(6) 以降、スイッチ スマート ライセンスがサポートされます。

DCNM でスイッチ スマート ライセンスを有効にするには：

- 自由形式の CLI 設定を使用して、スイッチでスマート ライセンス機能を有効にします。
- スイッチで **feature license smart** または **license smart enable** コマンドを使用して、スイッチのスマート ライセンスを構成します。
- license smart register **idtoken** コマンドを使用して、デバイスのトークンをスマート アカウントにプッシュします。DCNM の **[EXEC]** オプションを使用して、トークンをプッシュします。詳細については、[DCNM での EXEC モード コマンドの実行（Running EXEC Mode Commands in DCNM）]を参照してください。

ライセンスのないスイッチの場合、ライセンスは次の優先度に基づいて割り当てられます。

1. DCNM スマート ライセンス
2. DCNM サーバ ライセンス
3. DCNM 評価ライセンス

サーバ ライセンス ファイル

Cisco DCNM Web UI から、**[管理（Administration）]>[ライセンスの管理（Manage Licensing）]>[DCNM]>[サーバ ライセンス ファイル（Server License Files）]** を選択します。次のテーブルには Cisco DCNM

フィールド	説明
ファイル名	ライセンス ファイル名を指定します。
特長	ライセンス機能を指定します。
PID	製品 ID を指定します。
SAN (空き/合計)	SAN の無料ライセンス数と合計ライセンス数を表示します。
LAN (空き/合計)	LAN の無料ライセンス数と合計ライセンス数を表示します。
期限日（Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** フィールドのテキストで、7 日間で期限切れになるライセンスについては赤い色になっています。

Cisco DCNM ライセンスの追加

Cisco DCNM から Cisco DCNM ライセンスを追加するには、以下の手順を実行します。

Before you begin

次の手順を実行するには、ネットワーク管理者権限が必要です。

Procedure

ステップ 1 ライセンス ウィザードを開始するには**[管理（Administration）]>[ライセンスの管理（Manage Licensing）] > [DCNM]** を選択します。

ステップ 2 **[サーバ ライセンス ファイル（Server License Files）]** タブを選択します。

有効な Cisco DCNM-LAN [および DCNM-SAN（and DCNM-SAN）] ライセンス ファイルは表示されています。

ライセンスをロードするときは、セキュリティ エージェントが無効になっていることを確認してください。

ステップ 3 シスコから送付されたライセンス パック ファイルをローカル システムのディレクトリにダウンロードします。

ステップ 4 **[ライセンス ファイルの追加（Add License File）]** をクリックし、ローカル マシンに保存したライセンス パック ファイルを選択します。

ファイルはサーバ マシンにアップロードされ、サーバ ライセンス ディレクトリに保存されてから、サーバにロードされます。

Note .lic ファイルのコンテンツを編集しないようにしてください。編集すると、Cisco DCNM ソフトウェアでは、そのライセンス ファイルに関連付けられたすべての機能が無視されます。このファイルの内容に署名して、内容が変更されないようにする必要があります。ライセンス ファイルを間違って複数回コピー、名前変更、または挿入した場合、重複ファイルは無視されますが、元のファイルはカウントされます。

スイッチの機能：一括インストール

リリース 11.3（1）以降、Cisco DCNM では、1 つのインスタンスで複数のライセンスをアップロードできます。DCNM はライセンス ファイルを解析し、スイッチのシリアル番号を解析します。検出されたファブリックにライセンス ファイルのシリアル番号をマッピングして、各スイッチにライセンスをインストールします。ライセンス ファイルがブート フラッシュに移動され、インストールされます。

Cisco DCNM Web Client UI でスイッチにライセンスを一括インストールするには、次の手順を実行します。

1. **[管理 (Administration)] > [ライセンス付与の管理 (Manage Licensing)] > [スイッチ機能（Switch features）]** を選択します。

2. スイッチ ライセンス エリアで、**[ライセンス ファイルのアップロード（Upload License files）]** をクリックして適切なライセンス ファイルをアップロードします。

   一括でスイッチ ライセンスをインストール ウィンドウが表示されます。

3. ライセンスを選択で、**[ライセンスファイルの選択（Select License File file(s）]**をクリックします。

   ローカル ディレクトリにある適切なライセンス ファイルに移動して選択します。

   [開く（Open）] をクリックします。

4. DCNM サーバからスイッチにライセンス ファイルをコピーするためのファイル転送プロトコルを選択します。

   - ライセンス ファイルをアップロードするには、**TFTP**、**SCP**、または **SFTP** プロトコルのいずれかを選択します。

（注） すべてのプラットフォームですべてのプロトコルがサポートされているわけではありません。TFTP は、Win/RHEL DCNM SAN インストールでのみサポートされます。ただし、SFTP/SCP はすべてのインストール タイプでサポートされています。

5. **VRF** 設定をサポートするライセンスの VRF チェックボックスをオンにします。

   定義済みルートの 1 つの VRF 名を入力します。

6. **[スイッチでファイルを上書きする（Overwrite file on Switch）]** チェックボックスをオンにして、アップロードされた新しいライセンス ファイルでライセンス ファイルを上書きします。

（注） overwrite コマンドは、ブート フラッシュ内の既存のファイルに新しいファイルをコピーします。以前のライセンスがすでにインストールされている場合、それはインストールを上書きしません。

7. DCNM サーバ ログイン情報で、DCNM サーバのルート ユーザー名とパスワードを入力します。

   DCNM にアクセスするための認証ログイン情報を入力します。DCNM Linux 展開の場合、これはユーザー名です。OVA\ISO 展開の場合、**sysadmin** ユーザーの資格情報を使用します。

8. [アップロード（Upload）] をクリックします。

   ライセンス ファイルが DCNM にアップロードされています。次の情報がライセンス ファイルから抽出されます。

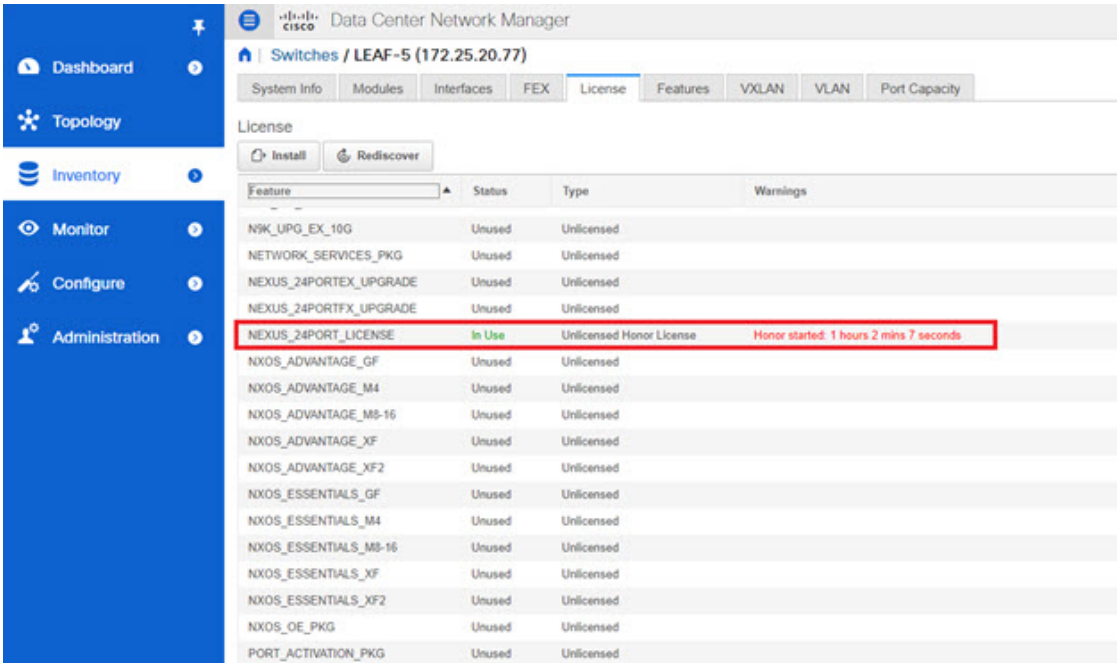
- スイッチ IP：このライセンスが割り当てられているスイッチの IP アドレス。
- ライセンス ファイル：ライセンス ファイルのファイル名
- 機能リスト：ライセンス ファイルでサポートされている機能のリスト

9. アップロードし、それぞれのスイッチにインストールするライセンスのセットを選択します。ライセンス ファイルは、単一の特定のスイッチに適用されます。
10. **[ライセンスのインストール（Install Licenses）]** をクリックします。

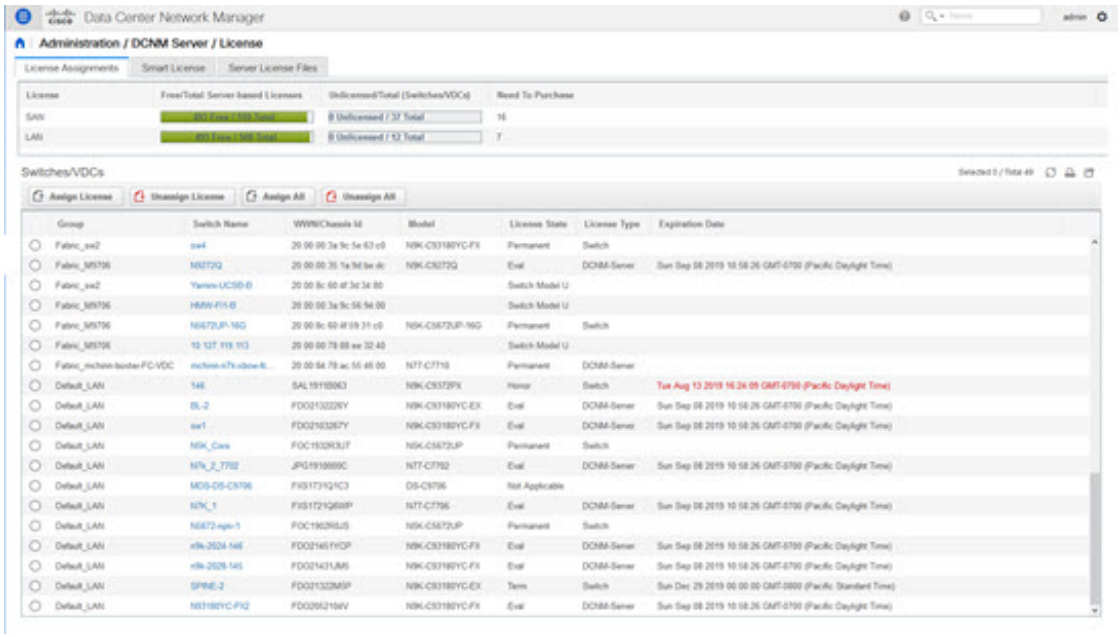
    選択したライセンスがアップロードされ、それぞれのスイッチにインストールされます。問題やエラーを含むステータスメッセージは、ファイルが完了するたびに更新されます。
11. ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ライセンスのステータス（License Status）]** テーブルにステータスが表示されます。

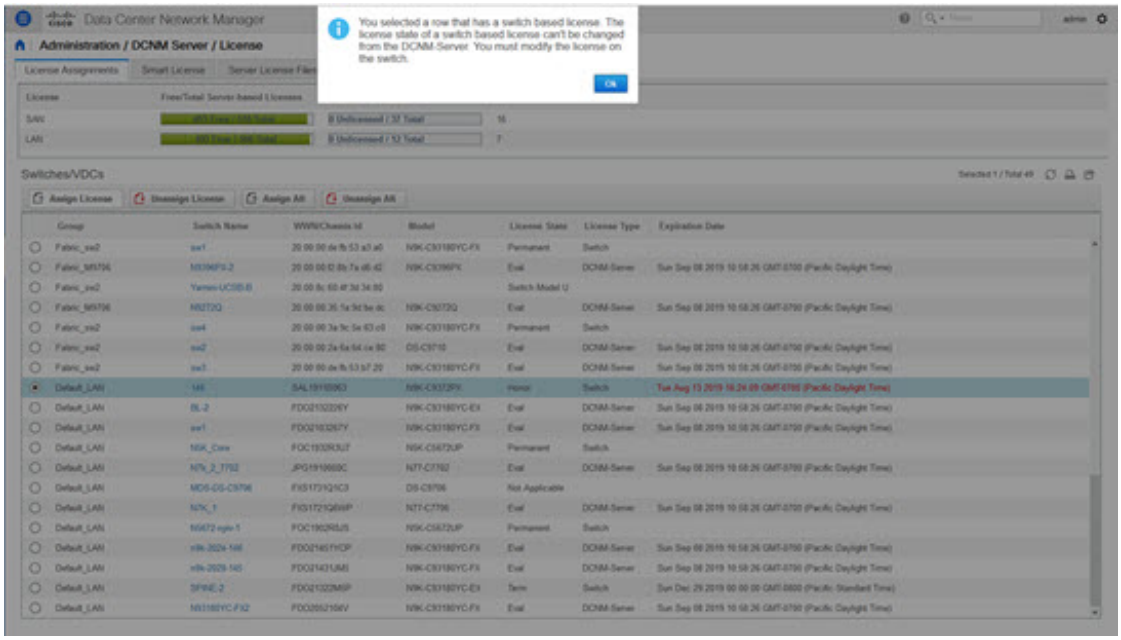
スイッチベースの名誉ライセンスのサポート

DCNM **Web UI** > **[インベントリ]** > **[スイッチ]** > **[ライセンス]** で、**[タイプ]** 列に「Unlicensed Honor License」と表示され、**[警告]** 列に **[Honor started: …]** と表示され、ライセンスが名誉モードに変更されてからの経過時間が表示されます。



（注） スイッチ ベースの優先ライセンスは、サーバ ベースのライセンス ファイルで上書きできません。





ユーザー管理

（注） DCNM にログインするたびに、DCNM サーバーは AAA 認証のために ISE サーバーから情報を取得します。最初のログイン後、ISE サーバは再度認証されません。

ユーザー管理メニューには、次のサブメニューがあります。

リモート AAA

Cisco DCNM Web UI からリモート AAA を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [リモート AAA プロパティ（Remote AAA Properties）]** を選択します。

AAA プロパティ構成ウィンドウが表示されます。

ステップ 2 ラジオ ボタンを使用して、次の認証モードのいずれかを選択します。

- ローカル：このモードでは、認証はローカル サーバーで認証されます。
- RADIUS：このモードでは、認証は指定された RADIUS サーバーに対して認証を行います。
- TACACS+：このモードでは、認証は指定された TACACS サーバーに対して認証を行います。
- スイッチ：このモードでは、認証は指定されたスイッチに対して認証を行います。
- LDAP：このモードでは、認証は指定された LDAP サーバーに対して認証されます。

ステップ 3 **[適用 (Apply)]** をクリックします。

ローカル

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[ローカル（Local）]** を選択します。

ステップ 2 **[適用（Apply）]** をクリックして認証モードを確認します。

RADIUS

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **Radius** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

TACACS+

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **TACACS+** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

Note IPv6 トランスポートの場合、フェールオーバーの状況中にアドレスの順序が変更されるため、AAA 認証の物理アドレスと VIP アドレスを入力します。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

スイッチ

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[スイッチ（Switch）]** を選択します。

DCNM は、IPv6 管理インターフェイスを備えた LAN スイッチもサポートします。

ステップ 2 プライマリ スイッチ名を指定し、**[適用（Apply）]** をクリックして認証モードを確認します。

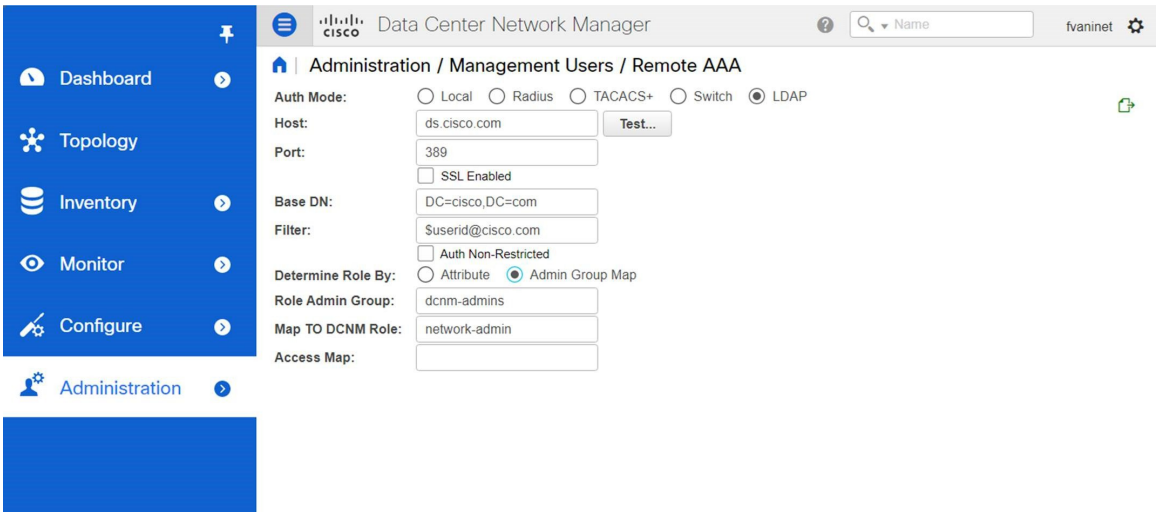
ステップ 3 (Optional) セカンダリおよびターシャリ スイッチの名前を指定します。

ステップ 4 **[適用（Apply）]** をクリックして認証モードを確認します。

LDAP

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[LDAP]** を選択します。



ステップ 2 **[ホスト（Host）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。

ドメイン ネーム システム（DNS）サービスが有効になっている場合は、LDAP サーバの DNS アドレス（ホスト名）を入力できます。

ステップ 3 [ポート（Port）] フィールドに、ポート番号を入力します。

非 SSL の場合は 389 を入力します。 SSL には 636 を入力します。デフォルトでは、ポートは非 SSL 用に構成されています。

ステップ 4 AAA サーバで SSL が有効になっている場合は、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにします。

Note LDAP over SSL を使用するには、ポートフィールドに **636** と入力し、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにする必要があります。

これで、LDAP クライアントに SSL セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの完全性と機密保持を保証します。

Note Cisco DCNM は、TLS を使用して LDAP サーバとのセキュアな接続を確立します。Cisco DCNM は、すべてのバージョンの TLS をサポートします。ただし、TLS の特定のバージョンは LDAP サーバによって決定されます。

たとえば、LDAP サーバがデフォルトで TLSv1.2 をサポートしている場合、DCNM は TLSv1.2 を使用して接続します。

ステップ 5 **[ベース DN（Base DN）]** フィールドに基本ドメイン名を入力します。

LDAP サーバはこのドメインを検索します。ベース DN は、DAP サーバで **dsquery.exe user -name**<*display_name*> コマンドを使用することで見つけることができます。

次に例を示します。

```
ldapserver# dsquery.exe users -name "John Smith"

CN=john smith,CN=Users,DC=cisco,DC=com
```

ベース DN は DC=cisco,DC=com です。

Note ベース DN 内の要素を正しい順序で入力していることを確認してください。これは、アクティブ ディレクトリ を照会するときのアプリケーションのナビゲーションを指定します。

ステップ 6 **[フィルタ処理（Filter）]** フィールドで、フィルタ処理 パラメータを指定します。

これらの値は、検索クエリをアクティブディレクトリに送信するために使用されます。LDAP 検索フィルタ文字列は最大 128 文字に制限されています。

次に例を示します。

- $userid@cisco.com

  これは、ユーザー プリンシパル名と一致します。

- CN=$userid、OU=従業員、OU=Cisco ユーザー

  これは、正確なユーザー DN と一致します。

ステップ 7 ロールを決定するオプションを選択します。**[属性（Attribute）]** または **[管理グループ マップ（Admin Group Map）]** のいずれかを選択します。

- **[管理グループ マップ（Admin Group Map）]**：このモードでは、DCNM はベース DN とフィルタ処理に基づいて、LDAP サーバにユーザーをクエリします。ユーザーがいずれかのユーザー グループに属している場合、DCNM ロールはそのユーザー グループにマッピングされます。
- **[属性（Attribute）]**：このモードでは、DCNM はユーザー属性をクエリします。属性を選択できます。**[属性（Attribute）]** を選択すると、**[ロール管理者グループ（Role Admin Group）]** フィールドが **[ロール属性（Role Attributes）]** に変わります。

ステップ 8 前の手順での選択に基づいて、**[ロール属性（Roles Attributes）]** または **[ロール管理者グループ（Role Admin Group）]** フィールドに値を入力します。

- **[管理グループ マップ（Admin Group Map）]** を選択した場合は、**[ロール管理グループ（Role Admin Group）]** フィールドに管理グループの名前を入力します。
- **[属性（Attribute）]** を選択した場合は、**[属性（Attribute）]** フィールドに適切な属性を入力します。

ステップ 9 **[DCNM ロールにマッピング（Map to DCNM Role）]** フィールドに、ユーザーにマッピングされる DCNM ロールの名前を入力します。

一般に、**network-admin** または **network-operator** が最も一般的なロールです。

次に例を示します。

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

この例では、Active Directory ユーザー グループ **dcnm-admins** を **network-admin** ロールにマップします。

複数の Active Directory ユーザー グループを複数のロールにマッピングするには、次のフォーマットを使用します：

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

[ロール管理グループ（Role Admin Group）] は空白で、**[DCNM ロールにマッピング（Map To DCNM Role）]** にはセミコロンで区切られた 2 つのエントリが含まれていることに注意してください。

ステップ 10 **[アクセス マップ（Access Map）]** フィールドに、ユーザーにマップするロール ベースのアクセスコントロール（RBAC）デバイス グループを入力します。

ステップ 11 **[テスト（Test）]** をクリックし、構成を確認します。[テスト AAA サーバ（Test AAA Server）] ウィンドウが表示されます。

ステップ 12 [テスト AAA サーバ（Test AAA Server）] ウィンドウに有効な**ユーザー名**と**パスワード**を入力します。

構成が正しい場合、次のメッセージが表示されます。

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

このメッセージは、[ロール管理グループ（Role Admin Group）] または [属性（Atribute）] モードに関係なく表示されます。これは、Cisco DCNM がクエリを Active Directory、グループ、およびロールにすることができ、を正しく構成できることを意味します。

テストが失敗すると、LDAP 認証に失敗したというメッセージが表示されます。

Warning テストが成功しない限り、構成を保存しないでください。間違った構成を保存すると、DCNM にアクセスできません。

ステップ 13 **[変更の適用（Apply Changes）]** アイコン（画面の右上隅にあります）をクリックして、構成を保存します。

ステップ 14 DCNM SAN サービスを再起動します。

- Windows の場合 – システムで、**[コンピュータの管理（Computer Management）] > [サービスとアプリケーション（Computer Management）] > [サービス（Services）]** に移動します。DCNM アプリケーションを見つけて右クリックします。**[停止（Stop）]** を選択します。1 分後、DCNM アプリケーションを右クリックし、**[開始（Start）]** を選択して DCNM SAN サービスを再起動します。

- Linux の場合 – **/etc/init.d/FMServer.restart** に移動し、リターン キーを押して DCNM SAN サービスを再起動します。

ローカル ユーザーを管理

管理者ユーザーとして、Cisco DCNM Web UI を使用して新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のグループまたは範囲を関連付けることができます。

この項の内容は、次のとおりです。

ローカルユーザーの追加

Procedure

ステップ 1 メニュー バーから**[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]**を選択します。**[ローカル ユーザー（Local Users）]** ページが表示されます。

ステップ 2 [ユーザの追加（Add User）] をクリックします。

[ユーザーを追加（Add User）] ダイアログボックスを表示します。

ステップ 3 **[ユーザー名（User name）]** フィールドにユーザー名を入力します。

Note ユーザー名は大文字と小文字が区別されますが、ユーザー名ゲストは予約済みの名前であり、大文字と小文字は区別されません。guest ユーザにできるのは、レポートの表示だけです。guest ユーザは guest パスワードを変更できず、DCNM Web クライアントの Admin オプションにもアクセスできません。

ステップ 4 **[ロール（Role）]** ドロップダウン リストからユーザーのロールを選択します。

ステップ 5 [Password] フィールドにパスワードを入力します。

Note SPACE 以外の全ての特殊文字はパスワードで許可されています。

ステップ 6 **[Confirm Password（パスワードの確認）]** フィールドで、パスワードを再入力します。

ステップ 7 **[Add（追加）]** をクリックすると、そのユーザーがデータベースに追加されます。

ステップ 8 ユーザーの追加を続行する場合は、ステップ 2 ～ 7 を繰り返します。

ローカル ユーザの削除

Cisco DCNM Web UI からローカル ユーザーを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザー（Local Users）] ページが表示されます。

ステップ 2 **[ローカル ユーザー（Local Users）]** テーブルから 1 人以上のユーザーを選択し、**[ユーザーの削除（Delete User）]** ボタンをクリックします。

ステップ 3 警告ウィンドウで **[はい（Yes）]** をクリックして、ローカル ユーザーを削除します。**[いいえ（No）]** をクリックし、削除をキャンセルします。

ユーザの編集

Cisco DCNM Web UI からユーザーを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

ステップ 2 チェックボックスを使用してユーザーを選択し、**[ユーザーの編集（Edit User）]**アイコンをクリックします。

ステップ 3 **[ユーザーの編集（Edit User）]** ウィンドウでは、デフォルトで**[ユーザー名（Username）]**と**[ロール（Role）]**が示されます。**[パスワード（Password）]** の指定と **[パスワードの確認（Confirm Password）]** をします。

ステップ 4 [適用（Apply）] をクリックし、変更を保存します。

ユーザ アクセス

ローカルユーザがアクセスできる特定のグループまたはファブリックを選択できます。これにより、ローカルユーザは、アクセスが許可されていない特定のグループまたはファブリックにアクセスできなくなります。これを行うには、次の手順を実行します。

Procedure

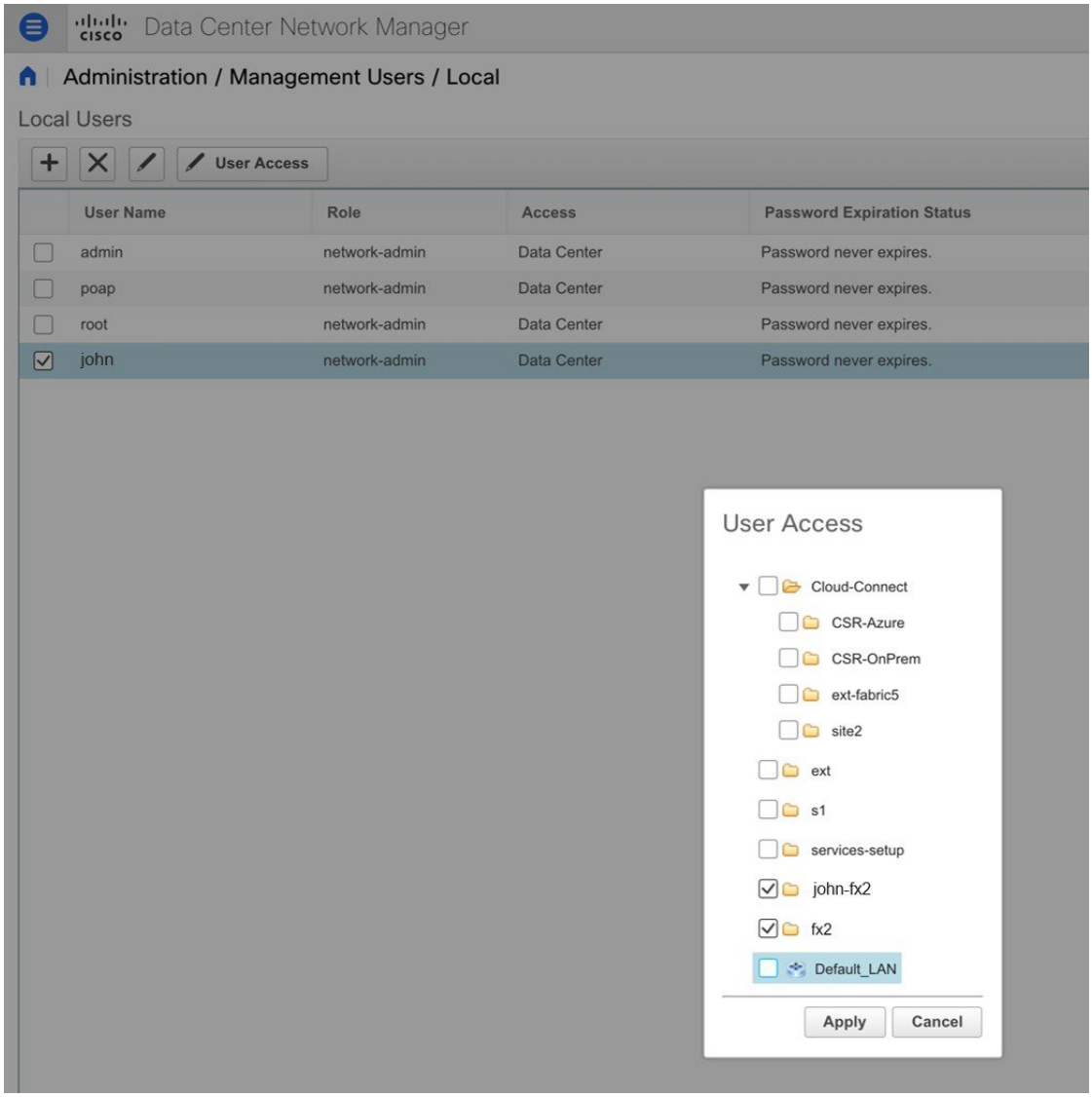
ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザ（Local Users）] ウィンドウが表示されます。

ステップ 2 **[ローカル ユーザ（Local Users）]** テーブルから一人のユーザを選択します。**[ユーザ アクセス（User Access）]** をクリックします。

[ユーザ アクセス（User Access）]選択ウィンドウが表示されます。

ステップ 3 ユーザがアクセスできる特定のグループまたはファブリックを選択し、**[適用（Apply）]** をクリックします。



クライアントを管理する

Cisco DCNM を使用して、DCNM クライアント サーバを切断できます。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [クライアント（Clients）]** を選択します。

DCNM サーバのリストが表示されます。

ステップ 2 チェックボックスを使用してDCNMサーバを選択し、**[クライアントの切断（Disconnect Client）]** をクリックして DCNM サーバを切断します。

Note 現在のクライアント セッションを切断することはできません。

パフォーマンスのセットアップ

パフォーマンスのセットアップ メニューには次のサブメニューが含まれます。

パフォーマンス セットアップ LAN 収集

Performance Manager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。Cisco DCNM を使用してパフォーマンス収集を追加または、削除することができます。スイッチの収集を作成する前に、スイッチにライセンスを付与し、**継続的な管理対象**状態に維持します。

Note Performance Manager データを収集するには、スイッチと DCNM サーバ間で ICMP ping を有効にする必要があります。**pm.skip.checkPingAndManageable** サーバ プロパティを true に設定してから、DCNM を再起動します。[Web **UI**]、**[管理（Administration）]**、**[DCNM サーバー（DCNM Server）]**、**[サーバーのプロパティ（Server Properties）]** の順に選択して、サーバ プロパティを設定します。

収集を追加する手順は、次のとおりです。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [LAN コレクション（LAN Collections）]** を選択します。

ステップ 2 ライセンスを取得したすべての LAN スイッチについて、チェック ボックスを使用して、**トランク**、**アクセス**、**エラーと破棄**、および**温度センサー**のパフォーマンス データ収集を有効にします。

ステップ 3 パフォーマンス データを収集する LAN スイッチのタイプを選択するためのチェックボックスをオンにします。

ステップ 4 [Apply] をクリックして、設定を保存します

ステップ 5 確認ダイアログボックスで、**[はい（Yes）]** をクリックして Performance Manager を再起動します。新しい設定を有効にするには、Performance Manager を再起動する必要があります。

Performance Manager SAN 収集

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。Cisco DCNM を使用してパフォーマンス コレクションを追加または、削除することができます。スイッチの収集を作成する前に、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。

収集を追加する手順は、次のとおりです。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [SAN 収集（SAN Collections）]** を選択します。

ステップ 2 ファブリックを選択して **[名前（Name）]**、**[ISL/NPV Links]**、**[ホスト（Host）]**、**[ストレージ（Storage）]**、**[FC フロー（FC Flows）]**、あるいは **[FC イーサネット（FC Ethernet）]** をこのデータ タイプのパフォーマンス収集を有効化するために選択します。

ステップ 3 [Apply] をクリックして、設定を保存します

ステップ 4 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。

パフォーマンス セットアップのしきい値

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。Cisco DCNM を使用してパフォーマンス コレクションを追加または、削除することができます。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、**managed Continuously** 状態に維持します。

Procedure

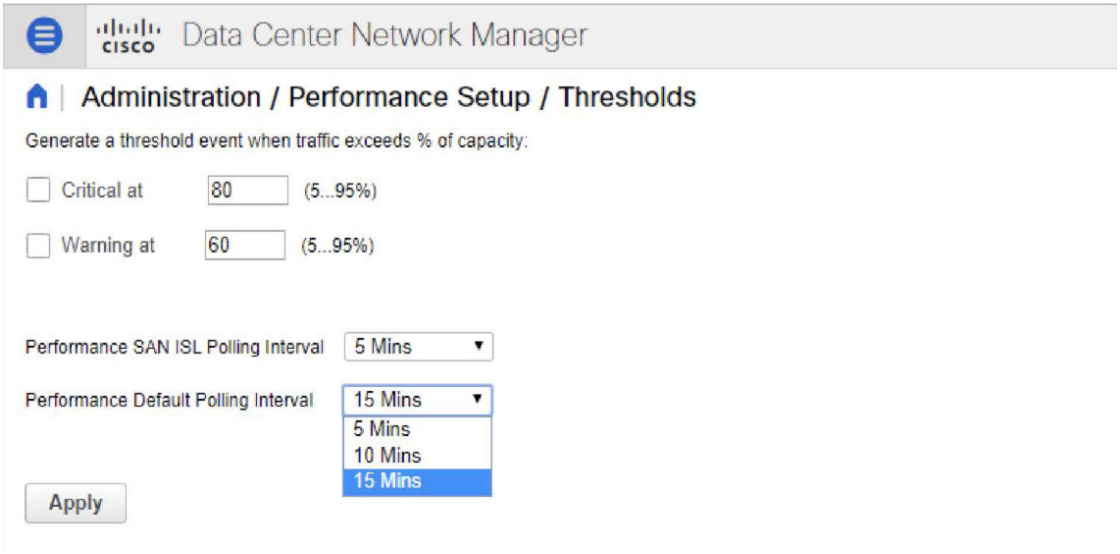
ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [しきい値（Thresholds）]** を選択します。

ステップ 2 **[トラフィックが容量の % を超えたときにしきい値イベントを生成します]** で、チェック ボックスを使用して **[重大になる時（Critical at）]** および **[警告が出る時（Warning at）]** の値を指定します。**[重大になる時（Critical at）]** の範囲は 5 ～ 95 で、デフォルトは 80 です。**[警告が出る時（Warning at）]** の範囲は 5 ～ 95 で、デフォルトは 60 です。

ステップ 3 ドロップダウン リストから **[パフォーマンス SAN ISL 投票間隔（Performance SAN ISL Polling Interval）]** の値を選択します。有効な値は、**5 分**、**4 分**、**3 分**、**2 分**、**1 分**、および **30 秒**です。デフォルトは **30 秒**です。

ステップ 4 ドロップダウン リストから **[パフォーマンス デフォルト投票間隔（Performance Default Polling Interval）]** の値を選択します。有効な値は、**5 分**、**10 分**、および **15 分**です。デフォルト値は **5 分**です。

ステップ 5 [適用（Apply）] をクリックします。



ユーザー定義の構成

Cisco DCNM Web UI からユーザー定義統計を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [ユーザー定義（User Defined）]** を選択します。

ユーザー定義の統計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。

[SNMP 統計をパフォーマンス収集に追加（Add SNMP Statistic to Performance Collection）] ウィンドウが表示されます。

ステップ 3 **[スイッチ（Switch）]** テーブルから、他の統計を追加するスイッチを選択します。

ステップ 4 **SNMP OID** ドロップダウン リストから、OID を選択します。

Note ドロップダウン リストから選択した SNMP OID ModuleX_Temp、IFHCInOctets.IFINDEX、IFHCOutOctest.IFINDEX の場合、「X」を正しいモジュール番号または対応する IFINDEX に置き換える必要があります。

ステップ 5 **[表示名（Display Name）]** ボックスに新しい名前を入力します。

ステップ 6 **[SNMP タイプ（SNMP Type）]** ドロップダウン リストから、タイプを選択します。

ステップ 7 **[追加（Add）]** をクリックすると、この統計が追加されます。

イベントのセットアップ

イベントのセットアップ メニューには次のサブメニューが含まれます。

イベント登録の表示

Syslog の送信、**トラップの送信**、および**トラップの遅延**を有効にするには、DCNM Web UI で次を設定する必要があります。

- **Syslog の送信**を有効にするには：**[Physical Attributes（物理的属性）] > [Events（イベント）] > [Syslog] > [Servers（サーバー）]** を選択します。**[行の作成]** をクリックし、必要な詳細を入力して、**[作成]** をクリックします。
- **送信トラップ**の有効化：**[物理属性（Physical Attributes）] > [イベント（Events）] > [SNMP トラップ（SNMP Traps）] > [送信先（Destination）]** を選択します。**[行の作成]** をクリックし、必要な詳細を入力して、**[作成]** をクリックします。
- **遅延トラップ**の有効化：**[物理属性] > [イベント] > [SNMP トラップ] > [遅延トラップ]** を選択します。**[機能の有効化]** 列で、チェック ボックスを使用してスイッチの遅延トラップを有効にし、遅延を分単位で指定します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [登録（Registration）]** を選択します。

SNMP および Syslog レシーバーと統計情報が表示されます。

ステップ 2 **[Syslog レシーバーを有効にする]** チェックボックスをオンにして **[適用]** をクリックすると、サーバー プロパティで Syslog レシーバーが無効になっている場合に有効になります。

イベント登録または syslog のプロパティを設定するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、画面の指示に従います。

ステップ 3 **[Syslog メッセージを DB にコピー（Copy Syslog Messages to DB）]**を選択し、**[適用（Apply）]** をクリックして syslog メッセージをデータベースにコピーします。

このオプションを選択しない場合、イベントは Web クライアントのイベント ページに表示されません。

2 番目のテーブルの列には、次の情報が表示されます。

- トラップを送信するスイッチ
- syslog を送信するスイッチ
- syslog アカウンティングを送信するスイッチ
- 遅延トラップを送信するスイッチ

通知の転送

Cisco DCNM Web UI を使用して、システム メッセージの通知転送の追加および削除を実行できます。

この項の内容は、次のとおりです。

通知転送の追加

Cisco DCNM Web UI は、電子メールまたは SNMPv1 トラップを介してファブリック イベントを転送します。

一部の SMTP サーバーでは、DCNM から SMTP サーバーに送信される電子メールに認証パラメータを追加する必要があります。Cisco DCNM リリース 11.4(1) 以降、DCNM により認証を必要とする任意の SMTP サーバーに送信される電子メールに認証パラメータを追加できます。この機能を構成するには、**[管理] > [DCNM サーバー] > [サーバー プロパティ]** ウィンドウで **[SMTP] > [認証]** プロパティを設定します。**server.smtp.authenticate** フィールドに **true** を入力し、**server.smtp.username** フィールドに必要なユーザー名を入力し、**server.smtp.password** フィールドに必要なパスワードを入力します。

Cisco DCNM Web UI からシステムメッセージの通知転送を追加および削除するには、次の手順を実行します。

Note テスト転送は、ライセンスされたファブリックに対してのみ機能します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

イベントの転送範囲、レシーバの電子メールアドレス、イベントの重大度、およびイベントのタイプが表示されます。説明の [正規表現（Regex）] フィールドは、転送送信元がイベントフォワーダの追加時に転送元が Syslog として選択されている場合にのみ適用されます。

ステップ 2 イベント転送を有効にするには、**[有効にする（Enable）]** チェックボックスをオンにします。

ステップ 3 **SMTP サーバー**の詳細と**送信元**電子メール アドレスを指定します。

ステップ 4 **[適用（Apply）]** をクリックして、設定を保存します。

ステップ 5 **イベント カウント フィルタ**で、イベント カウントのフィルタをイベント フォワーダーに追加します。

イベント カウントがイベント カウント フィルタで指定された制限を超えると、転送はイベントの転送を停止します。このフィールドでは、カウント制限を指定できます。イベントを転送する前に、Cisco DCNM はその発生がカウント制限を超えていないかどうかを確認します。その場合、イベントは転送されません。

ステップ 6 **[スヌーズ]** チェックボックスを選択して、**開始**日付と時刻、**終了**日付と時刻を指定します。**[適用（Apply）]** をクリックして、設定を保存します

ステップ 7 **[イベント フォワーダー ルール（Event Forwarder Rules）]** テーブルで、**[+]** アイコンをクリックしてイベント フォワーダー ルールを追加します。

[イベント フォワーダー ルールの追加（Add Event Forwarder Rule）] ダイアログ ボックスが表示されます。

ステップ 8 **[転送メソッド（Forwarding Method）]** で、**[電子メール（E-mail）]** または **[トラップ（Trap）]** を選択します。**[トラップ（Trap）]** を選択した場合は、ダイアログボックスに **[ポート]** フィールドが追加されます。

ステップ 9 **電子メール**転送メソッドを選択する場合は、**[電子メール アドレス（Email Address）]** フィールドに IP アドレスを入力します。**トラップ**メソッドを選択する場合は、**[アドレス（Address）]** フィールドにトラップの受信者の IP アドレスを入力し、ポート番号を指定します。

[アドレス（Address）] フィールドに IPv4 または IPv6 アドレスまたは DNS サーバー名を入力できます。

ステップ 10 **転送範囲（Forwarding Scope）** では、通知の**ファブリック/LAN** または**ポート グループ**を選択します。

ステップ 11 **[送信元]** フィールドで、**[DCNM]** または **[Syslog]** を選択します。

DCNM を選択すると、次のようになります。

a) **[タイプ（Type）]** ドロップダウン リストから、イベント タイプを選択します。

b) **[ストレージ ポートのみ（Storage Ports Only）]** チェックボックスをオンにして、ストレージ ポートのみを選択します。

c) **[最低重大度]** ドロップダウン リストから、受信するメッセージのシビラティ レベルを選択します。

d) **[追加（Add）]** をクリックして、通知を追加します。

[Syslog]を選択しと、次のようになります。

a) **[ファシリティ（Facility）]** リストから、syslog のファシリティを選択します。

b) syslog **タイプ**を指定します。

c) **[説明の正規表現（Description Regex）]** フィールドで、イベントの説明と一致する説明を指定します。

d) **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。

e) **[追加（Add）]** をクリックして、通知を追加します。

Note **[最低重大度（Minimum Severity）]** オプションは、**[イベント タイプ（Event Type）]** が [すべて（All）] に設定されている場合のみ使用できます。

Cisco DCNM が送信するトラップは、重大度タイプに対応しています。重大度タイプとともにテキストによる説明も提供されます。

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

通知の転送を削除する

通知の転送を削除できます。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

ステップ 2 削除する通知の前のチェックボックスを選択し、**[削除（Delete）]** をクリックします。

EMC CallHome の設定

Cisco DCNM Web UI から EMC がサポートする SAN スイッチの EMC Call Home を設定するには、次の手順を実行します。

Procedure

ステップ 1 **[管理] > [イベント セットアップ] > [EMC コール ホーム（EMC Call Home）]** を選択します。

ステップ 2 **[イネーブル化（Enable）]** チェックボックスを選択にして、この機能を有効にします。

ステップ 3 チェックボックスを使用して、ファブリックまたは個々のスイッチを選択します。

ステップ 4 一般的なメール情報を入力します。

ステップ 5 **[適用（Apply）]** をクリックして、E メール オプションを更新します。

ステップ 6 **[テストと適用（Apply and Test）]** をクリックして、E メール オプションを更新し、結果をテストします。

イベント抑制

Cisco DCNM では、ユーザー指定のサプレッサ ルールに基づいて、指定されたイベントを抑制することができます。このようなイベントは、Cisco DCNM Web UI および SAN クライアントには表示されません。イベントはDCNMデータベースに保持されず、電子メールまたはSNMPトラップを介して転送されません。

テーブルからサプレッサ ルールを表示、追加、変更、および削除できます。既存のイベント テーブルからサプレッサ ルールを作成できます。テンプレートとして特定のイベントを選択し、ルール ダイアログウィンドウを呼び出します。イベントの詳細は、イベント テーブルで選択したイベントから、ルール作成ダイアログ ウィンドウの入力フィールドに自動的に移植されます。

Note Cisco DCNM Web UI から EMC Call Home イベントを抑制することはできません。

このセクションの内容は次のとおりです。

イベント抑制ルールの追加

Cisco DCNM Web UI からイベント抑制にルールを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

[抑制（Suppression）] ウィンドウが表示されます。

ステップ 2 **[イベント抑制（Event Suppressors）]** テーブルの上にある **[追加（Add）]** アイコンをクリックします。

[イベント抑制ルールの追加（Add Event Suppressor Rule）] ウィンドウが表示されます。

ステップ 3 **[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ウィンドウで、ルールに **Name** を指定します。

ステップ 4 イベント送信元に基づくルールに必要な **[範囲（Scope）]** を選択します。

[範囲（Scope）] ドロップダウン リストには、LAN グループとポート グループが個別に表示されます。**[SAN][LAN ポート グループ（LAN, Port Groups）]** または **[任意（Any）]** を選択できます。**SAN** および **LAN**の場合は、ファブリックまたはグループまたはスイッチ レベルでイベントの範囲を選択します。**[ポート グループ（Port Group）]** 範囲のグループのみ選択できます。範囲として **[任意（Any）]** を選択する場合、抑制ルールはグローバルに適用されます。

ステップ 5 **Facility** 名を入力するか、**SAN/LAN Switch Event Facility** リストから選択します。

ファシリティを指定しない場合は、ワイルドカードが適用されます。

ステップ 6 ドロップダウン リストから、[イベント**Type**（Event）] を選択します。

イベント タイプを指定しない場合は、ワイルドカードが適用されます。

ステップ 7 **Description Matching** フィールドで、一致する文字列または正規表現を指定します。

ルール照合エンジンは、Java パターン クラスでサポートされている正規表現を使用して、イベントの説明テキストとの一致を検索します。

ステップ 8 **[アクティブ範囲（Active Between）]** ボックスをオンにして、イベントが抑制される有効な時間範囲を選択します。

デフォルトでは、時間範囲は有効になっていません。つまり、ルールは常にアクティブです。

Note 一般に、アカウンティングイベントを抑制しないでください。アカウンティングイベントの抑制ルールは、アカウンティング イベントが DCNM またはソフトウェアのスイッチのアクションによって生成される特定のまれな状況でのみ作成できます。たとえば、DCNMと管理対象スイッチ間のパスワード同期中に、多数の「*sync-snmp-password*」AAA syslog イベントが自動的に生成されます。アカウンティング イベントを抑制するには、**[抑制（Suppressor）]** テーブルに移動し、**[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ダイアログ ウィンドウを呼び出します。

Note **[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択して、既知のイベントの抑制ルールを作成します。アカウンティング イベントの抑制ルールを作成する際にショートカットはありません。

イベント抑制ルールを削除

Cisco DCNM Web UI からイベント抑制ルールを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 > イベントをセットアップ > 抑制（Administration > Event Setup > Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[Delete（削除）]**アイコンをクリックします。

ステップ 3 確認のために [はい（Yes）] をクリックします。

イベント抑制ルールの変更

イベント抑制ルールを変更するには、次のタスクを実行します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[編集（Edit）]** をクリックします。

[施設（Facility）]、**[タイプ（Type）]**、**[説明一致（Description Matching）]**文字列、および**[有効な時間範囲（Valid time range）]**を編集できます。

ステップ 3 **[適用（Apply）]** をクリックして、変更内容を保存します。

クレデンシャル管理

ユーザー ログイン情報管理メニューには、次のサブメニューがあります：

SAN 資格情報

Cisco DCNM ホームページで、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 資格情報（SAN Credentials）]** を選択すると、ファブリック シード スイッチへのSNMPアクセスの詳細が表示されます。ユーザーがすべてのファブリックへのアクセスを検証した場合は、ファブリックのすべてのシード スイッチの SNMP 資格情報が表示されます。

Cisco DCNM のスイッチ資格情報ウィンドウには、次のフィールドがあります。

フィールド	説明
Fabric Name（ファブリック名）	スイッチが属するファブリック名を表示します。

フィールド	説明
シード スイッチ	スイッチの IP アドレス。
[ユーザ名（User Name）]	Cisco DCNM のユーザーのユーザー名を指定します。
[パスワード（Password）]	スイッチ SNMP ユーザの暗号化形式を表示します。
SNMPv3 / SSH	SNMP プロトコルが検証されるかどうかを指定します。 デフォルト値は **false** です。
認証/プライバシー	認証プロトコルを指定します。 デフォルト値は **[NOT_SET]** です。
ステータス	スイッチのステータスを表示します

Cisco DCNM ユーザーが SNMP を使用してファブリックを設定する前に、ユーザーはファブリックのシード スイッチに SNMP 資格情報を提供し、検証する必要があります。ユーザーがファブリック シードスイッチの有効な資格情報を提供しない場合、[スイッチ クレデンシャル（Switch Credentials）] テーブルに SNMPv3/SSH および AuthPrivacy フィールドのデフォルト値が表示されます。

スイッチの行をクリックして、正しい資格情報を入力します。**[保存（Save）]**をクリックして変更内容を保存します。

ユーザーが構成を変更しても、有効なスイッチ資格情報を提供しない場合、ユーザーアクションは拒否されます。スイッチの資格情報を検証して、変更をコミットします。

この画面で次の操作を実行できます。

- 資格情報を再検証するには：
  1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 情報管理（SAN Credentials）]** を選択し、**[ファブリック名（Fabric Name）]** オプション ボタンをクリックして、資格情報を検証する必要があるシード スイッチを選択します。
  2. [再検証（Revalidate）] をクリックします。

     操作が成功したか失敗したかを示す確認メッセージが表示されます。

- スイッチ資格情報をクリアします。
  1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [SAN 情報管理（SAN Credentials）]** を選択し、**[ファブリック名（Fabric Name）]** オプション ボタンをクリックして、シード スイッチを選択し削除します。

2. [Clear] をクリックします。

   確認メッセージが表示されます。

3. **[はい（Yes）]** をクリックして、DCNM サーバからスイッチ資格情報を削除します。

LAN 資格情報

デバイス構成の変更中、Cisco DCNM はユーザーから提供されたデバイスの資格情報を使用します。ただし、LAN スイッチ資格情報がプロビジョニングされない場合、Cisco DCNM では **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** ページを開き、LAN 資格情報を構成するようにプロンプトが表示されます。

Cisco DCNM は、次の 2 つのログイン情報のセットを使用して ローカル エリア ネットワーク（LAN）デバイスに接続します。

- **[ディスカバリ資格情報（Discovery Credentials）]**：Cisco DCNM は、デバイスの検出および定期的なポーリング中にこれらのログイン情報を使用します。
- **[構成変更ログイン情報（Configuration Change Credentials）]**：ユーザーがデバイス構成を変更する機能を使用しようとすると、Cisco DCNM はこれらのログイン情報を使用します。

LAN ログイン情報管理では、構成変更ログイン情報を指定できます。LAN スイッチの構成を変更する前に、スイッチの構成変更 SSH ログイン情報を入力する必要があります。ログイン情報を提供しない場合、構成変更アクションは拒否されます。

これらの機能は、LAN ログイン情報機能からデバイス書き込みログイン情報を取得します。

- アップグレード（ISSU）
- メンテナンス モード（GIR）
- パッチ（SMU）
- テンプレートの展開
- POAP-Write erase reload、Rollback
- インターフェイスの作成/削除/設定
- VLAN の作成/削除/設定
- VPC ウィザード

デバイスが最初に検出されたかどうかに関係なく、構成変更のログイン情報を指定する必要があります。これは1回限りの操作です。ログイン情報が設定されると、構成変更操作に使用されます。

Default Credentials

デフォルトのログイン情報は、ユーザーがアクセスできるすべてのデバイスに接続するために使用されます。スイッチテーブルのデバイスそれぞれにログイン情報を指定して、デフォルトのログイン情報を上書きできます。

Note **[パスワード（Password）]**、**[パスワードの確認（Confirm Password）]** フィールドに適切なログイン情報を入力して **[保存（Save）]** をクリックした後、**[パスワードの確認（Confirm Password）]** フィールドが空白です。空白の **[パスワードの確認（Confirm Password）]** フィールドは、パスワードが正常に保存されたことを意味します。

Cisco DCNM はまず、[スイッチ（Switch）] テーブルの個別のスイッチログイン情報を使用しようとします。[スイッチ（Switch）] テーブルの資格情報（ユーザー名/パスワード）列が空白の場合、デフォルトのログイン情報が使用されます。

スイッチテーブル

スイッチテーブルは、ユーザーがアクセスしたすべてのローカルエリアネットワーク（LAN）スイッチをリストにします。デフォルトのログイン情報を上書きするスイッチログイン情報を個別に指定できます。ほとんどの場合、デフォルトのログイン情報のみを入力する必要があります。

この画面で次の操作を実行できます。

- ログイン情報の編集, on page 50
- ログイン情報の検証, on page 50
- スイッチログイン情報のクリア, on page 50
- リモート アクセスによる認証情報管理, on page 50

DCNM ユーザーの ローカル エリア ネットワーク（LAN）ログイン情報テーブルには、次のフィールドがあります。

フィールド	説明
スイッチ	ローカルエリアネットワーク（LAN）スイッチ名を表示します。
IP アドレス	スイッチの IP アドレスを指定します。
[ユーザ名（User Name）]	スイッチ DCNM ユーザーのユーザー名を指定します。
パスワード	SSH パスワードの暗号化形式を表示します。
グループ	スイッチが属するグループを表示します。

ログイン情報の編集

次のタスクを実行して、ログイン情報を編集します。

1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）資格情報（LAN Credentials）]** を選択し、ログイン情報を編集する必要がある **[スイッチ（Switch）]** チェック ボックスをオンにします。
2. [Edit] アイコンをクリックします。
3. スイッチに **[ユーザー名（User Name）]** および **[パスワード（Password）]** を指定します。

ログイン情報の検証

ログイン情報を検証するには、次のタスクを実行します。

1. **[管理（Administration）] > [ログイン情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN）ログイン情報（LAN Credentials）]** から、ログイン情報を検証する必要がある **[スイッチ（Switch）]** チェック ボックスを選択します。
2. [**Validate**] をクリックします。

   操作が成功したか失敗したかを示す確認メッセージが表示されます。

スイッチログイン情報のクリア

次のタスクを実行して、スイッチ ログイン情報をクリアします。

1. **[管理（Administration）] > [ログイン情報管理（Credentials Management）] > [ローカル エリア ネットワーク（LAN） ログイン情報（LAN Credentials）]**から、ログイン情報をクリアする必要がある **[スイッチ（Switch）]** チェック ボックスをオンにします。
2. [Clear] をクリックします。
3. **[はい（Yes）]** をクリックして、DCNM サーバからスイッチ ログイン情報をクリアします。

リモート アクセスによる認証情報管理

DCNM では、次のようなさまざまなモードでユーザーを認証できます。

- ローカル ユーザ ー- このモードでは、Cisco DCNM Web UI を使用して、新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のファブリックまたはグループへのアクセス権を提供できます。
- リモート ユーザー - このモードでは、DCNM にログインできます。DCNM サーバーは、AAA 認証のために、リモート認証サーバー（Cisco Identity Services Engine（ISE）など）から情報を取得します。シスコは、リモート認証用に TACACS+、RADIUS、および LDAP オプションをサポートしています。詳細については、「リモート AAA」を参照してください。

リモート認証用に DCNM を構成すると、AAA サーバーは認証と認可の両方を処理します。DCNM は、認証を確認するために入力されたユーザ ログインとパスワードを AAA サーバーに転送します。認証後、AAA サーバーは **cisco-avpair** 属性を介してユーザーに割り当てられた適切な権限/ロールを返します。この属性には、特定のユーザーがアクセスできるファブリックのリストを含めることができます。DCNM LAN 展開でサポートされるロールは次のとおりです。

- network-admin
- network-operator

デバイス検出資格情報と LAN 資格情報はどちらもデバイスへの書き込みアクセス権を提供しますが、書き込み操作は LAN 資格情報でのみ実行されるため、両者は異なります。デバイス検出資格情報は各デバイスに関連付けられ、デバイスを DCNM にインポートするときに 1 回だけ入力されます。DCNM は、デバイスへの SSH アクセスと SNMPv3 アクセスを組み合わせて使用する定期的な再検出に、これらの資格情報を使用します。ただし、LAN 資格情報は、ユーザーごとにすべてのユーザーに対して構成されます。適切なロールを持つユーザーが DCNM にアクセスする場合、そのユーザーは LAN 資格情報を入力してデバイスへの書き込みアクセス権を取得できます。書き込み操作では、LAN 資格情報を使用してデバイスにアクセスします。これにより、すべてのユーザーが DCNM で行った変更と、その結果としてデバイスに加えられた変更の適切な監査証跡が得られます。

TACACS+ や RADIUS などのリモート認証方式を使用して DCNM を設定する場合、ユーザーは次のように LAN 資格情報を構成できます。

- 通常の AAA リモート認証
- AAA リモート認証パススルー メカニズム
- DCNM サービス アカウントを使用した AAA リモート認証

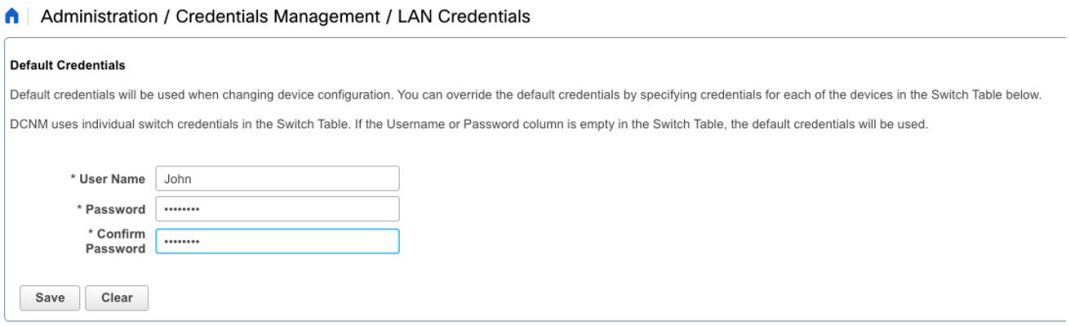
通常の AAA リモート認証

認証後、適切なロールを持つユーザーが初めて DCNM にログインすると、DCNM はユーザーに LAN 資格情報の入力を求めます。前述のように、DCNM はこれらの資格情報を使用して、デバイスへの書き込みアクセス権を提供します。すべてのユーザーは、このプロセスに従う必要があります。社内のビジネス ポリシーにより、ユーザーは 3 ～ 6 か月ごとにパスワードを変更する必要があるとします。次に、すべてのユーザーは、DCNM **[LAN 資格情報（LAN Credentials）]** ウィンドウでデバイスにアクセスするためのパスワードを更新する必要があります。また、AAA サーバーでパスワードを更新する必要があります。

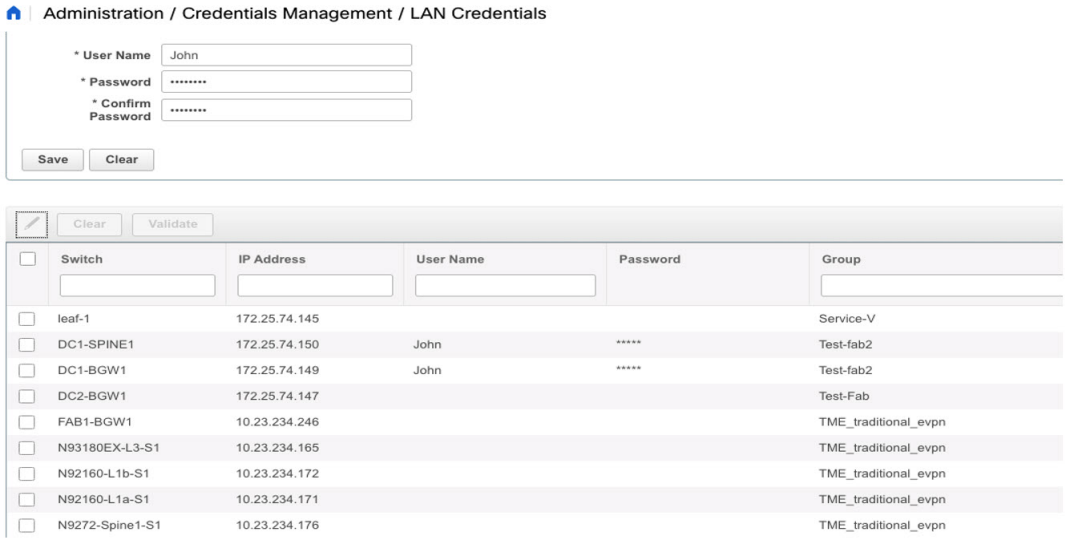
たとえば、ISE サーバーで認証を行う John という名前のユーザーについて考えてみましょう。

1. John は、自分のユーザー資格情報を使用して DCNM にログインします。
2. ISE サーバーは John のユーザー資格情報を認証し、DCNM は彼の LAN スイッチ資格情報を入力するためのメッセージを表示します。DCNM はこれらの資格情報を使用して、デバイスでさまざまな構成と書き込み操作を実行します。

3. John は、LAN スイッチの資格情報を入力します。DCNM は、すべてのデバイスで John によってトリガされるすべての書き込み操作に LAN スイッチ資格情報を使用します。ただし、John は、デバイスごとのアクセス ベースで LAN スイッチの資格情報を入力することを選択することもできます。このデバイスごとのアクセス オプションは、デフォルトの資格情報を入力することによって提供されるアクセスを上書きします。



John が再び DCNM にログインすると、DCNM は LAN スイッチ資格情報をすでにキャプチャしているため、LAN スイッチ資格情報を入力するためのメッセージを表示しません。John は、同じ資格情報を使用して、DCNM およびアクセス可能なデバイスにログインします。



4. ここで、数か月後に企業のITポリシーが変更されたとします。次に、Johnはリモート AAA サーバーで自分のパスワードを更新する必要があります。また、ステップ 3 を実行して、DCNM が LAN スイッチ資格情報を更新できるようにする必要があります。

したがって、このモードでは John が更新されたパスワードを使用して DCNM Web GUI にログインすると、DCNM は LAN 資格情報を入力するためのメッセージを表示しません。ただし、John は LAN 資格情報のパスワードを更新する必要があります。DCNM が新しく更新されたパスワードを継承し、デバイスで書き込み操作を実行できるようになるため、パスワードを更新する必要があります。

AAA リモート認証パススルー メカニズム

このモードでは、ユーザーがユーザー名とパスワードを入力して DCNM にログインすると、DCNM はそのユーザー資格情報をそのユーザーの LAN スイッチ資格情報設定のデフォルト資格情報に自動的にコピーします。その結果、ユーザーが初めてログインしたときに、DCNMは LAN スイッチ資格情報を入力するためのメッセージを表示しません。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。
2. `/root/directory`（**su** コマンドを使用）にログインします。
3. `/usr/local/cisco/dcm/fm/conf/server.properties` ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   dcnm.lanSwitch.sameUserAccount=true

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功すると、DCNM は LAN スイッチ資格情報を更新するためのメッセージを表示しません。これは、この情報がLANスイッチ資格情報に自動的にコピーされるためです。
8. 数か月後、企業の IT ポリシーが変更されることを考慮してください。このモードでは、John はリモート AAA サーバーでパスワードを更新する必要があります。その後、John が DCNM にログインすると、DCNM は更新された資格情報をユーザー John に関連付けられたデフォルトの LAN 資格情報に自動的にコピーします。

DCNM サービス アカウントを使用した AAA リモート認証

多くの場合、顧客は、共通のサービス アカウントを使用して DCNM コントローラから行われたすべての変更を追跡することを好みます。次の例では、ユーザーが DCNM コントローラを使用して変更を行い、デバイスに変更を加えています。これらの変更は、共通のサービスアカウントに対してデバイス上で監査ログに記録されます。したがって、コントローラによってトリガされた変更を、ユーザーがデバイス上で直接行った他の変更（アウトオブバンド変更とも呼ばれます）と区別することができます。アウトオブバンドの変更は、ユーザーアカウントから行われたデバイス アカウンティング ログに表示されます。

たとえば、リモート AAA サーバーに**ロボット**という名前のサービス アカウントを作成します。対応する資格情報を使用して、ロボット ユーザーは DCNM にログインできます。ロボット ユーザーは、デフォルトの LAN 資格情報を入力して、デバイスへの書き込みアクセス権を持つことができます。DCNM network-admin は、すべてのユーザーのデフォルトの LAN 資格情報を自動的に設定し、ロボットに関連付けられたデフォルトの LAN クレデンシャルを継承するサーバー プロパティを有効にします。

したがって、ユーザーが DCNM にログインして構成を変更すると、DCNM はロボットの LAN 資格情報を使用して変更をデバイスにプッシュします。DCNM 展開履歴ログは、変更をトリガしたユーザーを追跡し、DCNM からスイッチに展開された対応する変更をユーザー ロボットの監査ログで表示します。

DCNM でサービス アカウントを設定するには、次の手順を実行します。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。
2. `/root/ directory`（**su** コマンドを使用）にログインします。
3. `/usr/local/cisco/dcm/fm/conf/server.properties` ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   service.account=robot

（注） AAA パススルー アカウントまたはサービス アカウントのいずれかを有効にできます。

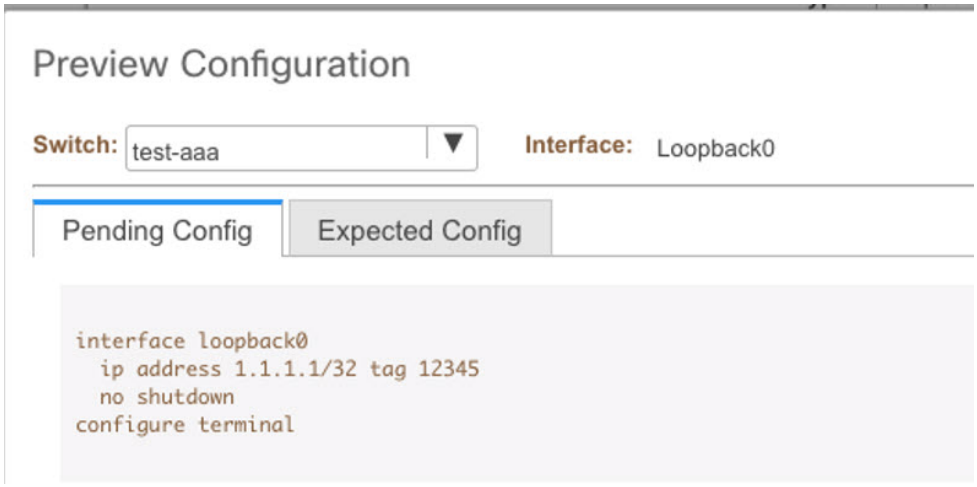
```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功した後、DCNM は LAN スイッチ資格情報を更新するためのメッセージを表示しません。ただし、John が **[LAN 資格情報（LAN Credentials）]** ページに移動すると、DCNM は、サービス アカウントが DCNM で有効になっているため、すべての LAN 資格情報がサービス アカウントから継承されることを示すメッセージを表示します。

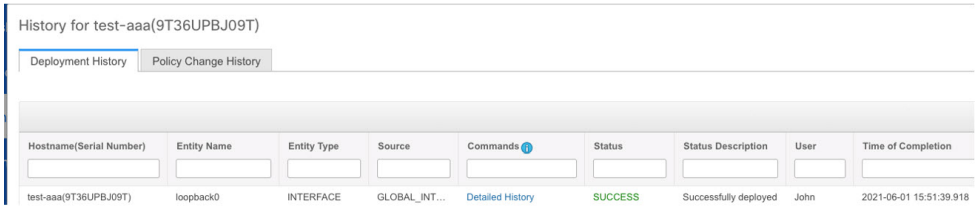
サービス アカウント構成監査

次のワークフローの例では、DCNM サービスアカウント機能の使用中に構成監査を検証できます。ただし、サービスアカウントのアクティブ化手順を完了している必要があります。

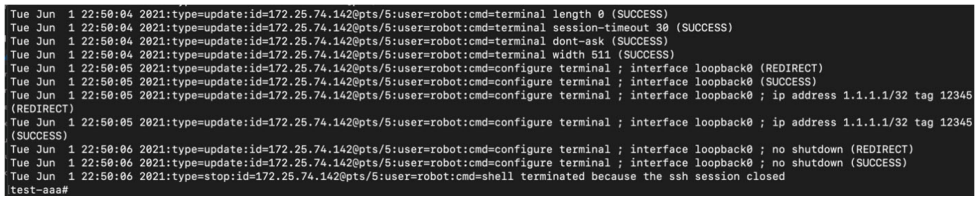
1. John は、デバイスでテスト ループバックを作成します。



2. John は、DCNM を使用して構成を展開します。
3. DCNM 展開の履歴により、John が最近の構成変更を行ったことを確認できます。



4. デバイスのアカウンティングログは、DCNM サービスアカウント（つまり、この例ではロボット）が NX-OS デバイスの変更をトリガしたことを示しています。



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。