管理

この章は次のトピックで構成されています。

- DCNM サーバ （1 ページ）
- ライセンスの管理 （26 ページ）
- ユーザー管理 （46 ページ）
- パフォーマンスのセットアップ （55 ページ）
- イベントのセットアップ （56 ページ）
- クレデンシャル管理 （62 ページ）

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。

- 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] > [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。

オーバーレイ展開のデフォルト ファブリック

リリース 11.4(1) 以降、Cisco DCNM カスタマイズでは、有効なファブリックの 1 つをデフォルトとして選択できます。この機能は、Cisco DCNM LAN ファブリック展開でのみ使用できます。

Cisco DCNM Web UI ですべてのオーバーレイ展開のデフォルト ファブリックを設定するには、次の手順を実行します。

（注） デフォルトファブリックの構成を使用できるのは、**ネットワーク管理者**ロールを持つユーザーのみです。

1. **[管理（Administration）] > [DCNM サーバー] > [カスタマイズ（Customization）]** を選択します。
2. **[オーバーレイ展開のデフォルト ファブリック（Default Fabric for Overlay Deployments）]** ドロップダウン リストで、すべてのオーバーレイ展開のデフォルトとして設定するファブリックの設定を選択します。

3. **[保存]** をクリックして、ファブリックをデフォルトとして設定します。

   デフォルトファブリックが正常に更新されたことを確認するメモがウィンドウの右下に表示されます。

4. デフォルトのファブリックを削除するには、ドロップダウンリストから **--select as オプション**を選択し、**[保存（Save）]** をクリックします。

ネットワーク基本設定

リリース 11.5（1）より前の **appmgr update network-properties** コマンドでは、ネットワークプロパティを変更できます。リリース 11.5（1）以降、Cisco DCNM では、Web UI からいくつかのネットワーク パラメータを変更できます。これらを変更すると、以前に構成されたパラメータが上書きされます。

[Cisco DCNM **Web UI] > [管理（Admin）] > [DCNMサーバ（DCNM Server）] > [カスタム化（Customization）] > [ネットワーク基本設定（Network Preferences）]** を選択して、DNS、NTP、および eth1/eth2 インターフェイスを変更します。

DNS

ドメイン ネーム システム（DNS）フィールドに、ドメイン ネーム システム（DNS）の IP アドレスを入力します。IPv6 アドレスを使用して DNS サーバを設定することもできます。複数のドメイン ネーム システム（DNS）サーバを構成できます。IP アドレス間の差別化要因としてコンマ (,) を使用します。

Note Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

NTP

[NTP サーバー (NTP Server)] フィールドに、NTP サーバーの IP アドレスを入力します。値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

ルート

インバンド (eth2)

[インバンド ネットワーク (In-Band Network)] 領域で、インバンド ネットワークの IPv4 アドレスおよびゲートウェイ IPv4 アドレスを入力します。DCNM が IPv6 ネットワーク上にある場合は、 IPv6 アドレス と ゲートウェイ IPv6 アドレス の関連する IPv6 アドレスを入力することで、ネットワークを構成します。

Note Nexus ダッシュボード サーバが DCNM 11.5(1) からサイトを追加する場合、データ ネットワーク経由で DCNM サーバに到達する必要があります。DCNM データ ネットワーク接続は、DCNM サーバの eth2 インターフェイスを介して定義されます。 DCNM のインバンド接続インターフェイスとも呼ばれます。Nexus ダッシュボードのデータ ネットワーク接続を使用した DCNM の eth2 接続が複数のサブネットにまたがっている場合、つまり、それらがレイヤ 3 ルートで接続されている場合、ND にサイトを追加する前に DCNM にルートを追加する必要があります。ダッシュレットのインバンド (eth2) 入力を介して ND データ ネットワークへのルートを入力します。

インバンド ネットワークにより、前面パネルのポートを介してデバイスへ到達可能になります。

[帯域外 (eth1)（Out-of-Band (eth1)）]

アウトオブバンド ネットワーク エリアで、IPv4 アドレスと ゲートウェイ IPv4 アドレスを入力します。DCNMがIPv6ネットワーク上にある場合は、IPv6アドレスとゲートウェイIPv6アドレスに関連するIPv6アドレスを入力して、ネットワークを設定します。

アウトオブバンド管理では、デバイス管理ポート (通常 mgmt0) への接続を提供します。

ログ情報の表示

Performance Manager、、SME サーバー、Web レポート、Web サーバー、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。

リリース 11.2(1) 以降、DCNM OVA および DCNM ISO のインストールでは、.log 拡張子を持つすべてのログ ファイルもリストされます。

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。

バックアップ構成ファイルは、次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

保持できるアーカイブ ファイルの数は **[デバイスあたり保持できる# アーカイブ ファイルの数：（# Number of archived files per device to be retained:）]** フィールドで設定されています。Cisco DCNM LAN ファブリックのインストールでは、バックアップはデバイスごとではなく、ファブリックごとに取得されます。バックアップ ファイルの数がフィールドに入力された値を超えると、バックアップの最初のバージョンが削除され、最新バージョンに対応します。たとえば、フィールドに入力された値が **50** の場合、ファブリックの 51 番目のバージョンがバックアップされると、最初のバックアップ ファイルが削除されます。

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。

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。

ネイティブ HA

Before you begin

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。

Procedure

ステップ 1 デフォルトでは、DCNM は組み込みデータベース エンジン PostgreSQL にバンドルされています。ネイティブ DCNM HA は、**アクティブ/ウォーム スタンバイ**として実行されている 2 つの DCNM によって実現され、組み込みデータベースはリアルタイムで同期されます。アクティブ DCNM がダウンすると、スタンバイは同じデータベースデータを引き継ぎ、操作を再開します。スタンバイ ホスト データベースの停止シナリオは、この手順の後に文書化されます。

ステップ 2 メニュー バーから、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [ネイティブ HA（Native HA）]** を選択します。

ネイティブ HA ウィンドウが表示されます。

ステップ 3 **[フェールオーバ（Failover）]**ボタンをクリックしてから**[OK]**をクリックすると、スタンバイ ホストへの DCNM の手動フェールオーバを許可できます。

- または、Linux コンソールからこのアクションを開始することもできます。

  a. DCNM アクティブ ホストに SSH で接続します。

  b. 「/usr/share/heartbeat/hb_standby」と入力します。

ステップ 4 **[強制同期（Force Sync）]** をクリックし、**[OK]** をクリックすると、データベースとディスク ファイルをスタンバイ ホストに手動で同期することができます。

ステップ 5 **[テスト（Test）]** をクリックしてから **[OK]** をクリックすると、HA セットアップをテストまたは検証できます。

What to do next

このサブセクションでは、いくつかのHAトラブルシューティング シナリオについて説明します。

スタンバイ ホスト データベースがダウンしています：通常、DCNMデータベース（PostgreSQL）はアクティブ ホストとスタンバイ ホストでアップしていますDCNM 10.1 以前のバージョンでは、データベース同期の失敗によりスタンバイ データベースがダウンする場合があります。

- 「ps -ef | grep post」と入力します。複数の postgres プロセスが実行されていることがわかります。そうでない場合は、データベースがダウンしていることを示しています。
- データベース同期の開始時に作成されたバックアップ ファイルからデータベース データを復元します。ディレクトリを「/usr/local/cisco/dcm/db」に変更します
- ファイル replication/ pgsql-standby-backup.tgz の存在を確認します。ファイルが存在する場合は、データベース データ ファイルを復元します。

```
rm -rf    data/*
tar -zxf    replication/ pgsql-standby-backup.tgz    data
/etc/init.d/postgresql-9.4 start
ps -ef | grep post
```

アクティブな DCNM ホストは、2 つのデータベースを同期します。

TFTP サーバはアクティブ ホストの eth1 VIP アドレスにバインドされていません : TFTP サーバはアクティブ ホスト (スタンバイ ホストではなく) で実行する必要があり、eth1 VIP アドレスにバインドする必要があります。一部のセットアップでは、TFTP 設定ファイルによるとバインドアドレスが VIP アドレスではないため、スイッチが TFTP を使用しようとしたときに問題が発生する可能性があります。

- 「grep bind /etc/xinetd.d/tftp」と入力して、TFTP 設定ファイルに正しいバインド アドレスがあるかどうかを確認します。表示された IP アドレスが eth1 VIP アドレスでない場合は、バインド アドレスを VIP アドレスに変更します。新しいスタンバイ ホストに対してこの手順を繰り返します。バインド アドレスを VIP アドレスに更新します。
- アクティブ ホストで " " /etc/init.d/xinetd restart" と入力して、TFTP を再起動します。

Note TFTP サーバーは、「appmgr start/stop ha-apps」コマンドで開始または停止できます。

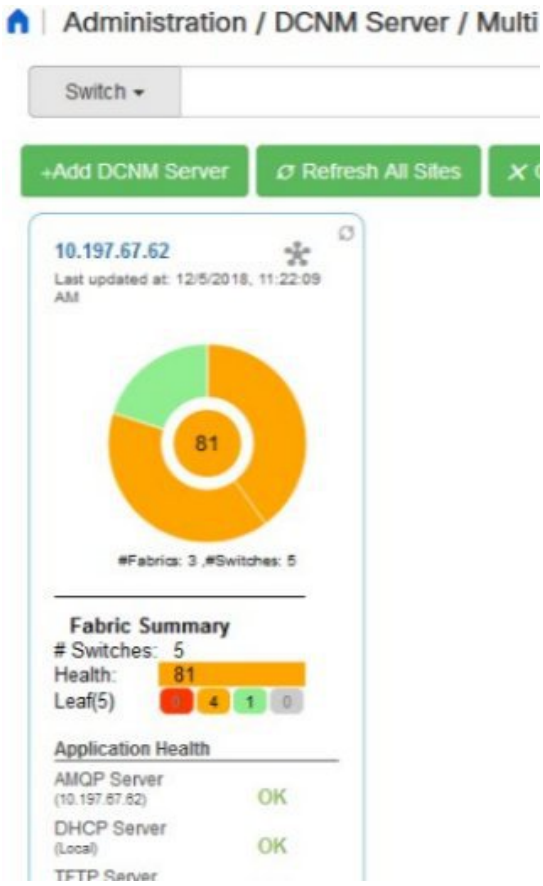
マルチ サイト マネージャ

Multi Site Manager を使用すると、DCNM サーバ アプリケーションの状態を表示し、ローカル サイトとリモート サイトのスイッチのスイッチ情報を取得できます。リモート DCNM サーバのスイッチ情報にアクセスするには、そのサーバを Multi Site Manager に登録する必要があります。リモート DCNM サーバにアクセスし、スイッチ情報を検索する手順について説明します。

リモート DCNM サーバ情報の追加

この手順により、現在ログオンしている DCNM サーバからリモート サイトの DCNM サーバにアクセスできます。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 サイトでの登録が必要です。

1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。Multi Site Manager 画面が表示されます。



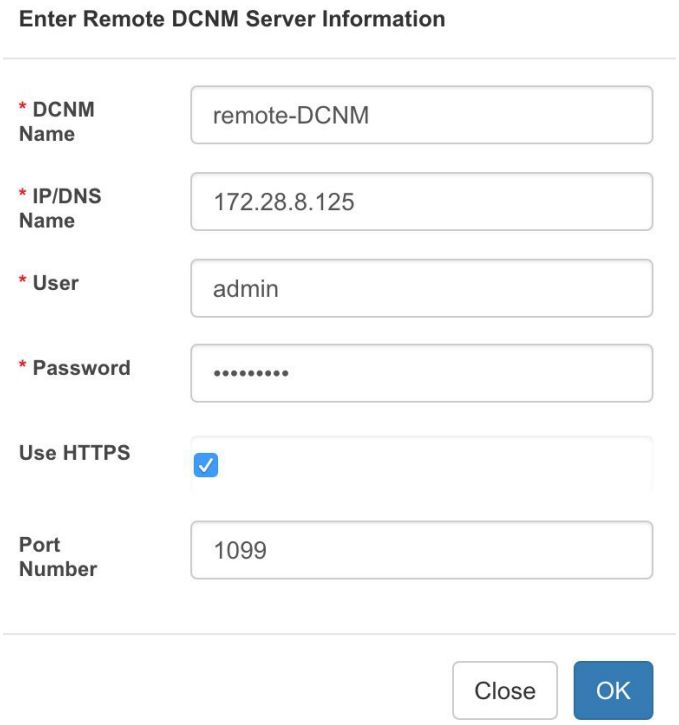
現在ログオンしている DCNM アプリケーションのヘルス ステータスが画面に表示されます。

Note **アプリケーション ヘルス**機能は、DCNM ISO/OVA インストール タイプでのみ使用でき、Windows/RHEL インストール タイプでは使用できません。

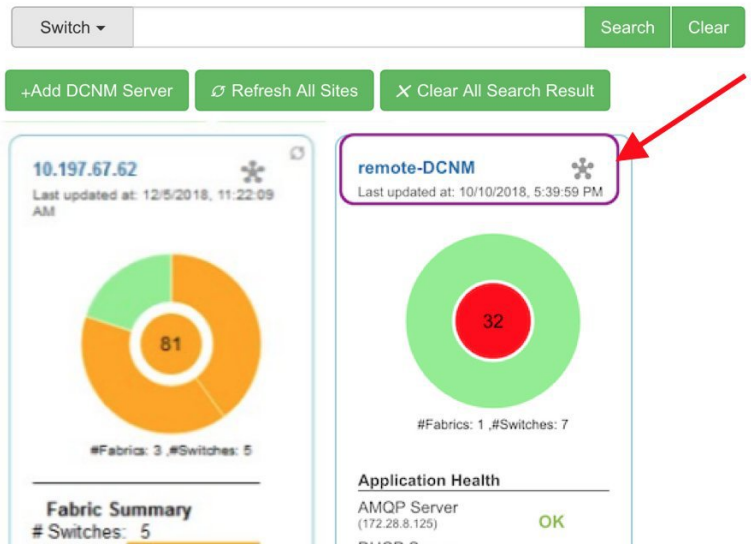
2. **[+ DCNM サーバの追加（+Add DCNM Server）]** をクリックします。**[リモート DCNM サーバ情報の入力（Enter Remote DCNM Server Information）]** 画面が表示されます。

   リモート DCNM サーバ名、その IP アドレスまたは URL、リモート DCNM サーバのユーザ クレデンシャル、およびオプションでポート番号を入力します。

Note **[HTTPS を使用（Use HTTPS）]** チェック ボックスを無効にしないでください。無効にすると、DCNM にアクセスできなくなります。



3. [OK] をクリックします。検証後、リモート DCNM サーバが画面のローカル DCNM サーバの隣に表示されます。



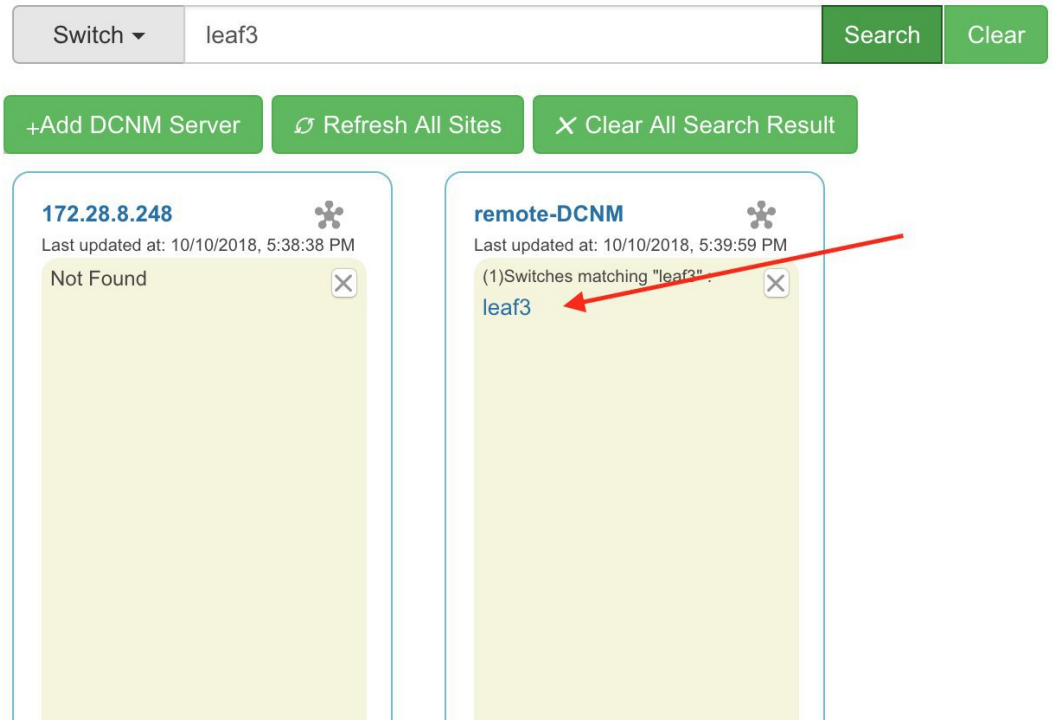
[すべてのサイトを更新（Refresh All Sites）] をクリックして、更新された情報を表示できます。

スイッチ情報の取得

1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。Multi Site Manager 画面が表示されます。
2. 画面上部の検索ボックスから、次のいずれかのパラメータに基づいてスイッチを検索します。
   - VM 情報（**[VM IP]** および **[VM 名（VM Name）]**フィールド）：接続された VM の IP アドレスまたは名前。
   - スイッチ情報（**[スイッチ（Switch）]**および**[MAC]**フィールド）：スイッチの名前または MAC アドレス。
   - スイッチ上に存在するセグメント（**[セグメント ID（Segment ID）]** フィールド）。

   一致する場合、スイッチ名は適切なローカルまたはリモート DCNM サーバの図の検索ボックスの下にハイパーリンクとして表示されます。

   この例では、スイッチ **leaf3** は、DCNM サーバによって管理されるリモート サイトで使用できます。**Leaf3** へのリンクは、**リモート DCNM** パネルで使用できます。



3. **Leaf3** をクリックして、隣接するブラウザタブに詳細なスイッチ情報を表示します。

   いつでも、**[トポロジ ビューの開始（Launch Topology View）]** アイコンをクリックして、ファブリックのトポロジを表示できます。

デバイス コネクタ

デバイスコネクタは、クラウドベース管理プラットフォームであるCisco Intersightの機能を実現する組み込み管理コントローラです。

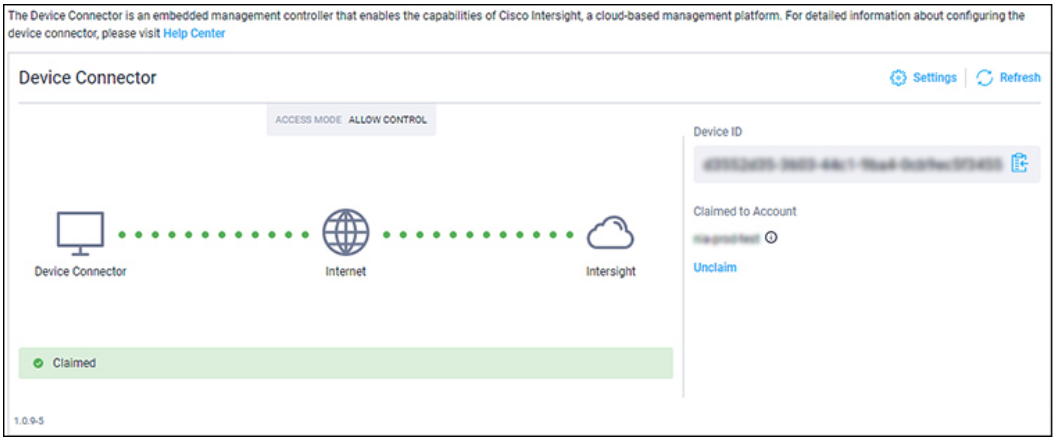
Networks Insights アプリケーションは、Cisco DCNM プラットフォームの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight クラウド ポータルに接続されます。Cisco Intersight は、Network Insights アプリケーションを介してデバイスを管理およびモニタするのに役立つ仮想アプライアンスです。デバイス コネクタは、接続されている DCNM に対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

デバイス コネクタの構成

Cisco DCNM Web UI からデバイス コネクタを構成するには、次の手順を実行します。

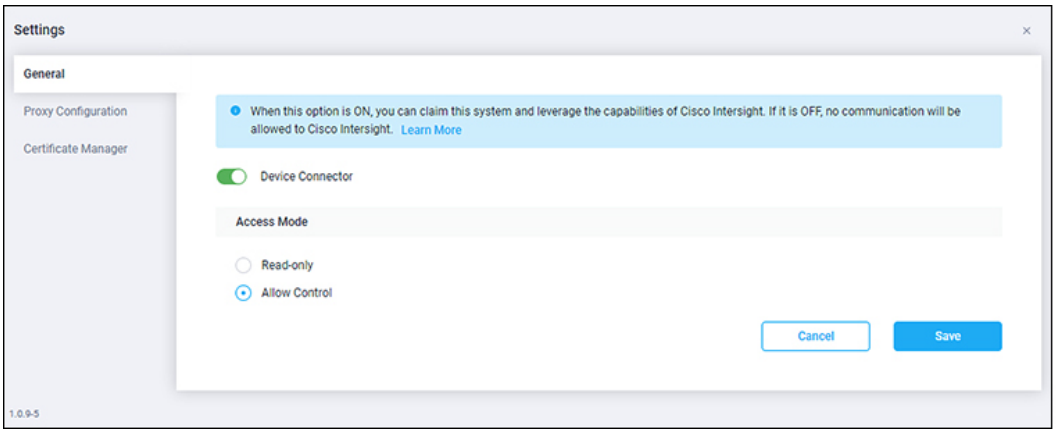
1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [デバイス コネクタ（Device Connector）]** を選択します。

   [デバイス コネクタ（Device Connector）] 作業ウィンドウが表示されます。



2. [設定（Settings）] をクリックします。

   [設定 - 全般（Settings - General）] ウィンドウが表示されます。



- **デバイス コネクタ（スイッチ）**

  これは、Cisco Intersight とのデバイス コネクタ通信のメイン スイッチです。スイッチがオンの場合（緑色のハイライト）、デバイス コネクタはシステムを要求し、Cisco Intersight の機能を活用します。スイッチがオフの場合（灰色の強調表示）、Cisco DCNM と Cisco Intersight の間で通信を行うことができません。

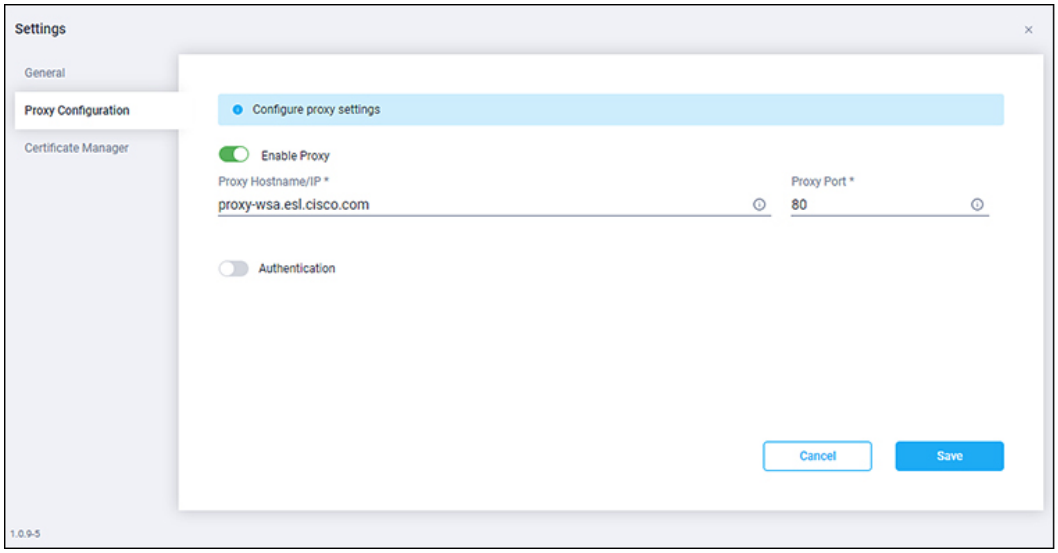
- **アクセス モード**

  - **[読み取り専用（Read-only）]**：このオプションは、Intersight からこのデバイスに変更が加えられないことを保証します。たとえば、ファームウェアのアップグレードやプロファイルの展開などのアクションは読み取り専用モードでは許可されません。ただし、アクションは特定のシステムで使用可能な機能によって異なります。

  - **[制御を許可（Allow Control）]**：このオプション（デフォルトで選択）を使用すると、Cisco Intersight で使用可能な機能に基づいて、クラウドからすべての読み取り/書き込み操作を実行します。

3. [デバイス コネクタ（Device Connector）] をオン（緑のハイライト）に設定し、**[制御を許可（Allow Control）]** を選択します。
4. **[プロキシ構成（Proxy Configuration）]** をクリックします。

   [設定 - プロキシ構成（Settings - Proxy Configuration）] ウィンドウが表示されます。



- **プロキシを有効にする（スイッチ）**

  [HTTPS プロキシ（HTTPS Proxy）] を有効にしてプロキシを構成します。

（注） Network Insights にはプロキシ設定が必要です。

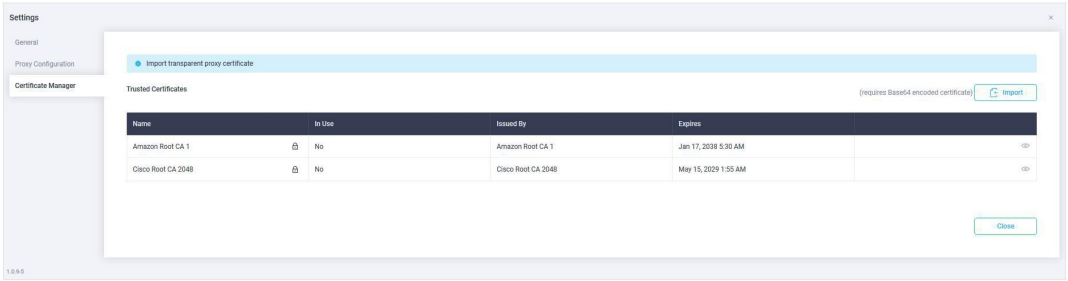
- **プロキシ ホスト名/IP* およびプロキシ ポート***：プロキシ ホスト名または IP アドレス、およびプロキシ ポート番号を入力します。
- **認証（スイッチ）**

  認証を通じてプロキシアクセスを有効にします。スイッチがオンの場合（緑色のハイライト）、プロキシ サーバへの認証が必要です。スイッチがオフ（灰色のハイライト）の場合、認証は必要ありません。

  ユーザー名*とパスワード：認証用のユーザー名とパスワードを入力します。

  デバイス コネクタには必須のログイン クレデンシャルのフォーマットはないので、入力したクレデンシャルがそのまま構成済み HTTP プロキシ サーバに渡されます。ドメイン名でユーザー名を限定する必要があるかどうかは、HTTP プロキシ サーバーの構成によって異なります。

5. プロキシを有効にし（緑色のハイライト）、ホスト名とポート番号を入力します。
6. （オプション）プロキシ認証が必要な場合は、それを有効にして（緑色のハイライト）、ユーザー名とパスワードを入力します。
7. [保存（Save）] をクリックします。
8. **[証明書マネージャ（Certificate Manager）]** をクリックします。



信頼できる証明書がテーブルに表示されます。

信頼できる証明書の一覧が表示されます。有効な信頼できる証明書をインポートできます。

- **[インポート（Import）]**

  ディレクトリを参照し、CA 署名付き証明書を選択してインポートします。

（注） インポートされた証明書が ***.pem（base64 エンコード）** 形式である必要があります。

- 次の情報と証明書のリストを表示することができます。
  - **[名前 (Name)]**—CA 証明書の共通名。

- **[使用中（In Use）] -** トラストストアで証明書を正常にリモート サーバの確認に使用されたかどうか。
- **[Issued By]**: 証明書の発行認証局。
- **[Expires]**—証明書の有効期限。

（注） バンドルされた証明書は削除できません。

スイッチの NX API 証明書管理

Cisco NX-OS スイッチを NX-API HTTPS モードで機能させるには、SSL 証明書が必要です。SSL 証明書を生成し、CA によってそれに署名することができます。スイッチ コンソールで CLI コマンドを使用して、証明書を手動でインストールできます。

リリース 11.4(1) から、Cisco DCNM では、NX-API 証明書を DCNM にアップロードするための Web UI フレームワークを提供しています。後で、DCNM によって管理されるスイッチに証明書をインストールできます。

この機能は、Cisco DCNM OVA/ISO 展開でのみサポートされます。

（注） この機能は、Cisco NXOS バージョン 9.2(3) 以降で動作するスイッチでサポートされます。

データセンター管理者は、スイッチごとにASCII（base64）エンコードの証明書を生成します。この証明書は、次の 2 つのファイルで構成されます。

- 秘密キーを含む `.key` ファイル
- 証明書を含む `.crt/.cer/.pem` ファイル

Cisco DCNM は、組み込みキー ファイル、つまり `.crt/.cer/.pem` ファイルを含む単一の証明書ファイルもサポートします。これには、.key ファイルのコンテンツも含めることができます。

DCNM は、バイナリ エンコードされた証明書はサポートしていません。つまり、`.der` 拡張子の証明書はサポートされません。キー ファイルは、暗号化用のパスワードで保護できます。Cisco DCNM は暗号化を義務付けていません。ただし、これは DCNM に保存されるため、キー ファイルを暗号化することをお勧めします。DCNM は AES 暗号化をサポートします。

CA 署名付き証明書または自己署名証明書のいずれかを選択することができます。Cisco DCNM は署名を義務付けていません。ただし、セキュリティ ガイドラインでは、CA 署名付き証明書を使用することを推奨しています。

複数のスイッチ用に複数の証明書を生成して、DCNM にアップロードすることができます。証明書に適したスイッチを選択できるように、証明書に適切な名前を付けてください。

1 つの証明書と対応するキーファイルをアップロードすることも、複数の証明書とキーファイルを一括アップロードすることもできます。アップロードが完了したら、スイッチにインストールする前に、アップロード リストを確認することができます。組み込みキー ファイルを含む証明書ファイルがアップロードされた場合、DCNM は自動的にキーを取得します。

証明書とキーファイルは同じファイル名である必要があります。たとえば、証明書ファイル名が `mycert.pem` の場合、キーファイル名は `mycert.key` である必要があります。証明書とキー ペアのファイル名が同じでない場合、DCNM はスイッチに証明書をインストールできません。

Cisco DCNM では、スイッチに証明書を一括インストールできます。一括インストールでは同じパスワードが使用されるため、すべての暗号化キーは同じパスワードで暗号化する必要があります。キーのパスワードが異なる場合、証明書を一括モードでインストールすることはできません。一括モードインストールでは、暗号化されたキー証明書と暗号化されていないキー証明書を一緒にインストールできますが、すべての暗号化キーは同じパスワードを持つ必要があります。

スイッチに新しい証明書をインストールすると、既存の証明書が新しい証明書に置き換えられます。

同じ証明書を複数のスイッチにインストールすることができます。ただし、一括アップロード機能は使用できません。

（注） DCNM は、提供される証明書またはオプションが有効であることを要求しません。この規則に従うかどうかは、ユーザーとスイッチの要件次第です。たとえば、スイッチ 1 のための証明書が生成されても、それがスイッチ 2 にインストールされた場合、DCNM は証明書の適用を強制しません。スイッチは、証明書のパラメータに基づいて証明書を受け入れるか、拒否するかを選択できます。

[Cisco **DCNM Web UI] > [管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** に、次のテーブルが表示されます。

- **[証明書インストール ステータス（Certificate Installation Status）]** テーブル：スイッチに最後にインストールされた証明書のステータスを表示します。また、証明書が以前に更新された時刻も表示されます。
- **[DCNM にアップロードされた証明書（Certificates Uploaded to DCNM）] テーブル**：DCNM およびスイッチ アソシエーションにアップロードされた証明書を表示します。

  ただし、証明書とスイッチの関連付けを確認するには、証明書のインストール ステータスの表を参照してください。アップロードテーブルは、DCNM に証明書をアップロードし、スイッチにインストールするためだけのものです。

また、スイッチ NX-API SSL 証明書管理機能の使用方法を示すビデオを見ることもできます。ビデオ：NX-API SSL 証明書管理の切り替えを参照してください。

DCNM での証明書のアップロード

Cisco DCNM Client Web UIを使用して証明書を DCNM にアップロードするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 適切なライセンス ファイルをアップロードするには **[DCNM にアップロードされた証明書（Certificates Uploaded to DCNM）]** エリア内にある **[証明書をアップロード（Upload Certificates）]** をクリックします。

ステップ 3 ローカル ディレクトリを参照し、DCNM にアップロードする必要がある証明書キーペアを選択します。

拡張子が .cer/.crt/.pem および .key の証明書を個別に選択できます。

Cisco DCNM では、埋め込みキーファイルを含む単一の証明書ファイルをアップロードすることもできます。キー ファイルはアップロード後に自動的に取得されます。

ステップ 4 **[開く (Open)]** をクリックし、選択したファイルを DCNM にアップロードします。

ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書は、**[DCNMにアップロードされた証明書（Certificates Uploaded to DCNM）]** エリアに表示されます。

[証明書のインストール ステータス（Certificate Installation Status）] エリアに、ステータスが **UPLOADED** である証明書が表示されます。

証明書がキーファイルなしでアップロードされた場合、ステータスは **KEY_MISSING** と表示されます。

スイッチでの証明書のインストール

Cisco DCNM Web UIを使用してスイッチに証明書をインストールするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 **[証明書のインストール ステータス（Certificate Installation Status）]** 領域で、証明書ごとに **[スイッチ（Switch）]** 列をクリックします。

ステップ 3 ドロップダウン リストから、証明書に関連付けるスイッチを選択します。

[保存（Save）] をクリックします。

ステップ 4 インストールする必要がある証明書を選択し、**[スイッチに証明書をインストール（Install Certificates on Switch）]** をクリックします。

複数の証明書を選択して、一括インストールを実行できます。

ステップ 5 **[一括証明書インストール（Bulk Certificate Install）]** ウィンドウで、証明書を DCNM にアップロードします。次の操作を行ってください。

一括インストール機能を使用して、同じインスタンスに最大 20 の証明書をインストールできます。

a) 証明書を DCNM にアップロードするためのファイル転送プロトコルを選択します。

証明書をアップロードするために、SCP または SFTP プロトコルを選択できます。

b) VRF 構成をサポートする証明書の VRF チェックボックスをオンにします。

スイッチが DCNM に到達するために使用する VRF 名を入力します。一般に、DCNM にはスイッチの管理 VRF を介して到達しますが、DCNM に到達するために使用されるスイッチで構成されている任意の VRF に到達できます。

c) NX-API 証明書資格情報に、証明書の生成時にキーを暗号化するために使用したパスワードを入力します。

証明書とともにアップロードされたキーが暗号化されていない場合は、このフィールドを空のままにします。

1 回の一括インストールで、暗号化されていないキーと暗号化されたキーおよび証明書をインストールできることに注意てください。ただし、暗号化キーに使用するキーパスワードを指定する必要があります。

d) [インストール（Install）] をクリックします。

証明書が特定のスイッチに正常にインストールされたかどうかを確認する通知メッセージが表示されます。

証明書のインストール ステータス エリアで、証明書のステータスに「**インストール済み**」が表示されるようになりました。

証明書のリンク解除と削除

証明書をスイッチにインストールすると、DCNM は DCNM から証明書をアンインストールできません。ただし、スイッチにはいつでも新しい証明書をインストールできます。スイッチにインストールされていない証明書は削除できます。スイッチにインストールされている証明書を削除するには、スイッチから証明書のリンクを解除してから、DCNM から削除する必要があります。

（注） スイッチから証明書のリンクを解除しても、スイッチの証明書は削除されません。証明書はまだスイッチに存在します。Cisco DCNM はスイッチの証明書を削除できません。

Cisco DCNM Web UI を使用してDCNM レポジトリから証明書を削除するには、以下の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 **[証明書のインストール ステータス（Certificate Installation Status）]** 領域で、削除する必要がある証明書を選択します。

ステップ 3 **[クリア（Clear）]** 認証書をクリックします。

確認メッセージが表示されます。

ステップ 4 **[OK]** をクリックして、選択した証明書をクリアします。

ステータス カラムには [UPLOADED] と表示されます。[Switch] カラムには [NOT_INSTALLED] と表示されます。

ステップ 5 証明書を選択し、**[証明書のクリア（Clear Certificates）]** をクリックします。

証明書が [証明書のインストール ステータス（Certificate Installation Status）] テーブルから削除されます。

ステップ 6 DCNMエリアにアップロードされている証明書で、スイッチから現在、リンク解除されている証明書を選択します。

[証明書を削除（Delete Certificates）]をクリックします。

証明書は DCNM から削除されます。

NX API 証明書管理のトラブルシューティング

証明書のインストール中にエラーが発生することがあります。次のセクションでは、スイッチの NX-API 証明書管理のトラブルシューティングについて説明します。

COPY_INSTALL_ERROR

問題文 : エラー メッセージ COPY_INSTALL_ERROR

理由 Cisco DCNM がスイッチに到達できません。

解決策 :

- スイッチが Cisco DCNM から到達可能かどうかを確認します。SSH ログインを実行し、スイッチに ping を実行して確認できます。
- スイッチは、その管理インターフェイスを介して DCNM に接続します。スイッチ コンソールから DCNM に ping できるかどうかを確認します。スイッチが VRF を必要とする場合、正しい vrf が提供されている場合。
- 証明書の秘密鍵が暗号化されている場合は、正しいパスワードを指定してください。
- 正しいキー ファイルが証明書とともにアップロードされていることを確認します。証明書ファイルとキー ファイルが同じファイル名であることを確認します。

CERT_KEY_NOT_FOUND

問題文：Error message CERT_KEY_NOT_FOUND

理由：証明書（.cer、.crt、.pem）のアップロード中にキー ファイルがアップロードされませんでした。

解決策：

- 証明書（.cer、.crt、または.pem）ファイルとそれに対応する .key ファイルのファイル名が同じであることを確認します。

  例：証明書ファイル名が mycert.crt の場合、キー ファイルも mycert.key である必要があります。

- DCNM はキー ファイルを証明書ファイル名で識別します。したがって、キー ファイルは同じファイル名にする必要があります。
- 証明書とキー ファイルを同じファイル名でアップロードし、証明書をインストールします。

DCNM のバックアップ

Cisco DCNM リリース 11.5（1） から、Cisco DCNM Web UI からスケジュールされた DCNM バックアップをトリガーできます。Web UI からバックアップをトリガすると、**appmgr backup** コマンドが実行されます。**[バックアップ（Backup）]** ウィンドウの **[サーバ バックアップ ジョブ（Server Backup Jobs）]** タブに、次の情報が表示されます。

Table 1: サーバ バックアップ ジョブ タブ

パラメータ	説明
ノード	バックアップがアクティブかスタンバイかを指定します。スタンドアロン ノードの場合、ローカルパスとして表示されます。 **Note** HA クラスタの場合、1 つのアクティブ ノードと 1 つのスタンバイ ノードが作成されます。ただし、HA クラスタにはアクティブ ノードのみを選択できます。
スケジュール	スケジュールされたバックアップがいつトリガーされるかを指定します。
ローカルパス	バックアップが保存されるローカル パスを指定します。
リモート宛先	バックアップが保存されるユーザー名、ホストIP、およびリモート宛先を指定します。バックアップをリモートの場所に保存しない場合は空です。 **Note** バックアップのコピーもローカルパスに保存されます。
ログパス	ログエントリが保存されるパスを指定します。この情報を使用して、問題をトラブルシューティングできます。
保存されたバックアップ	バックアップのバージョン数を指定します。デフォルト値は 5 です。

[バックアップ（Backup）] ウィンドウで次のアクションを実行できます。

バックアップの作成

Cisco DCNM ウェブ UI からバックアップを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [追加（Add）] をクリックします。

[バックアップ スケジュールを作成（Create Backup Schedule）] ダイアログ ボックスが表示されます。

ステップ 3 **[スケジュール（schedule）]** 領域の **[開始時刻（Start At）]** ドロップダウン リストを使用して時間を選択します。

ステップ 4 バックアップの周波数を次から選択します。

有効なオプションは次のとおりです。

- **[毎日（Daily）]** : 毎日バックアップをトリガする場合は、このラジオ ボタンを選択します。
- **[毎週（Weekly）]** : 週に 1 回バックアップをトリガする場合は、このラジオ ボタンを選択します。このラジオ ボタンを選択すると、曜日を選択するオプションが表示されます。

ステップ 5 保存するバックアップの数を、**[宛先（Destination）]** エリアの下の **[保存されたバックアップの最大数（Max # of Saved Backups）]** フィールドに入力します。

最大 10 個のバックアップを保存でき、デフォルト値は 5 です。

ステップ 6 （任意） リモートの場所にバックアップを保存するには、**[リモートの宛先（Remote Destination）]** チェックボックスをオンにします。

[リモート処理接続先（Remote Destination）] チェックボックスをオンにすると、次のフィールドが使用可能になります。

フィールド	説明
User	ユーザ名を入力します。
[パスワード（Password）]	パスワードを入力します。 （注） DCNM とリモート ホスト間のキーレス構成を有効にしている場合は、パスワードを入力する必要はありません。
ホスト IP	DCNM に接続されているホストの IP アドレスを入力します。
パス	バックアップを保存するリモート処理の接続先パスを入力します。

（注）
- バックアップ ファイルは巨大で、サイズはギガバイトです。
- バックアップのコピーは常にローカルの接続先にも保存されます。

ステップ 7 [作成（Create）] をクリックします。

CLI を使用して **appmgr backup** コマンドを実行しても、**[バックアップ（Backup）]** ウィンドウにデータが入力されます。また、**appmgr backup schedule show** コマンドを使用して、CLI で Web UI からスケジュールしたバックアップを表示することもできます。

バックアップの変更

Cisco DCNM Web UI からバックアップを変更するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [変更（Modify）] をクリックします。

[バックアップ スケジュールの変更（Modify Backup Schedule）] ダイアログ ボックスが表示されます。

ステップ 3 必要な変更を加えます。

ステップ 4 [変更（Modify）] をクリックします。

バックアップを削除

Cisco DCNM ウェブ UI からバックアップを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [削除（Delete）] をクリックします。

確認用のダイアログボックスが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

（注） CLI で **appmgr backup schedule none** コマンドを実行すると、バックアップが削除されます。**[バックアップ（Backup）]** ウィンドウを更新すると、バックアップが削除されたかどうかを確認できます。

ジョブ実行の詳細

[バックアップ（Backup）] ウィンドウの **[ジョブ実行の詳細（Job Execution Details）]** タブに、次の情報が表示されます。

Table 2: **サーバのバックアップ スケジュール エリア**

パラメータ	説明
ノード	ノードがアクティブかスタンバイかを指定します。スタンドアロン ノードの場合、ローカル ノードとして表示されます。
ファイルのバックアップ	バックアップが保存されるパスを指定します。
Start Time	バックアップ プロセスが開始された時刻を指定します。
終了時刻	バックアップ プロセスが終了した時刻を指定します。
ログ ファイル	ログエントリが保存されるパスを指定します。この情報を使用して、問題をトラブルシューティングできます。
Status	バックアップが成功したか失敗したかを指定します。
エラーメッセージ	バックアップ中に表示されたエラー メッセージがあれば、それを指定します。

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またはローカルエリアネットワーク（LAN）を指定します。
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。

フィールド	説明
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 • Expired • 無効 • スマート
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、ツールバーで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。
ライセンスの割り当てを解除	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。
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表を更新し、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場合、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]** 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。

オナー ライセンス モード

リリース 11.3(1) から、Cisco DCNM 評価ライセンスの有効期間が 30 日から 60 日に延長されました。つまり、60日後です。すべてのライセンスには、有効期限が付いています。ライセンスの有効期限が切れると、Cisco DCNM では、ライセンスされたすべての機能を使用できるようになります。スイッチが再度ライセンスを付与されるか、ライセンスを手動で削除するまで、スイッチはオナーモードのままになります。

ライセンス オナー モードのスイッチがある場合、DCNM にログオンした後にエラー メッセージが表示されます。

```
**************************************
*Your licenses are out of compliance.
Your inventory contains switches that are unlicensed for DCNM Operation*

**************************************
```

[管理（Administration）] > [ライセンシングの管理（Manage Licensing）] > [DCNM] に移動し、**[スイッチ/VDC（Switches/VDCs）]** テーブルでスイッチを選択し、**[ライセンスの割当（Assign License）]** をクリックしてライセンスを更新します。

ガイドライン

- ライセンスが割り当てられていないスイッチは、ライセンスがないと見なされます。ライセンスのないスイッチは、ライセンスが必要な DCNM 機能を使用できません。

- スイッチに期限切れの EVAL ライセンスがある場合、EVAL から オナー モードに変更され、ライセンス機能は引き続き動作します。
- 期限切れの EVAL ライセンスをスイッチに割り当てることはできません。
- スイッチベースのオナー ライセンスを持つスイッチは、サーバーベースのライセンスで上書きすることはできません。
- 検出されたスイッチにライセンスが割り当てられていて、有効なライセンスが利用できない場合、有効期限付きの優先ベースのライセンスがスイッチに割り当てられます。

名誉モード ライセンスのナグ イベント

オナー モードのすべてのライセンスについて、7 日ごとにイベントが生成されますnag イベントは、ユーザーに「DCNM-SAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります」と通知します。または、「DCNM-LAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります。」

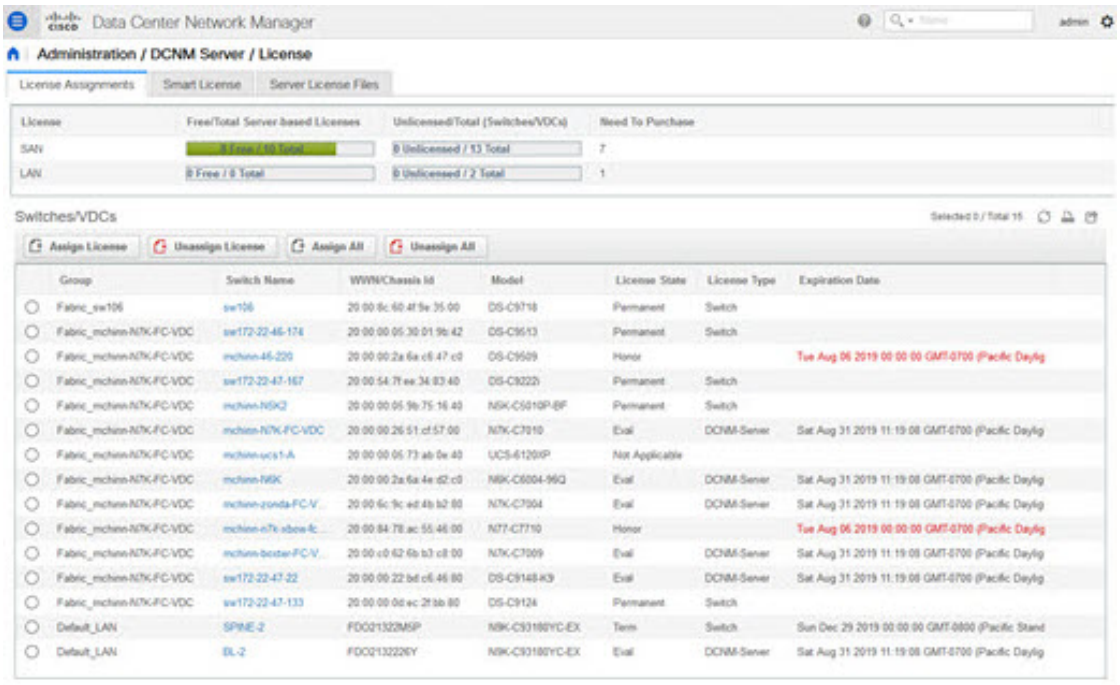
Cisco DCNM にログオンすると、追加のポップアップ通知が表示され、「DCNM-SAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります」という通知が表示されます。

サーバーベースのオナー ライセンスのサポート

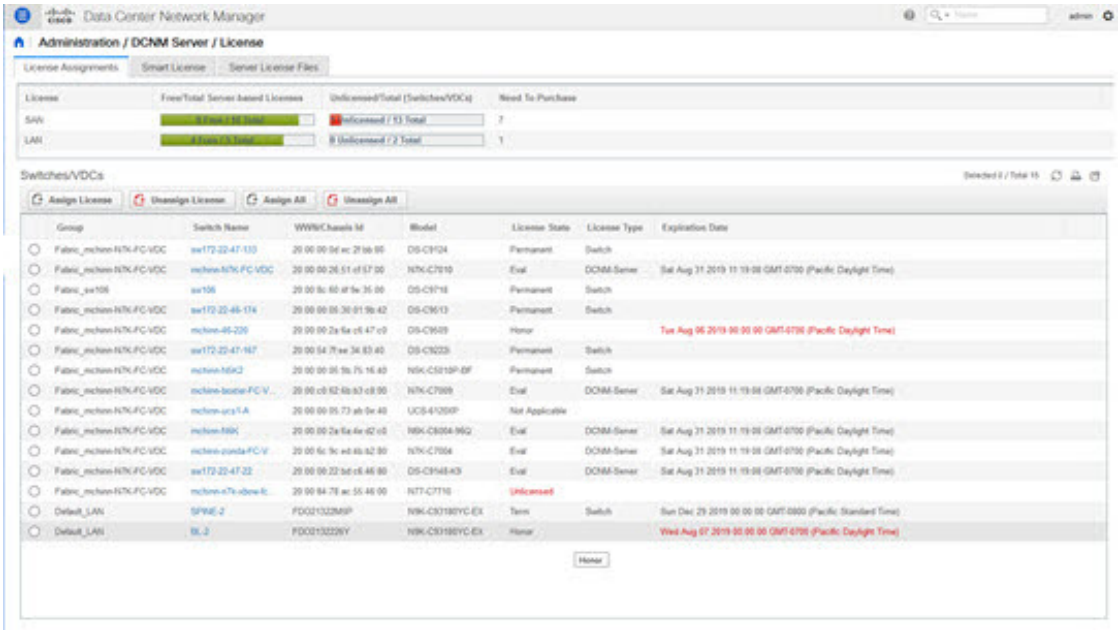
DCNM **Web UI > [管理] > [ライセンスの管理] > [DCNM]** で、**[ライセンスの状態]** 列に [名誉] が表示され、**[有効期限日]** 列に、ライセンスが期限切れになって**オナー** モードに変更された日時が表示されます。

スイッチは、再起動後もオナー モードのままになります。ライセンスをオナーモードから変更するには、ライセンスの割り当てを手動で解除するか、新しい有効なライセンスをスイッチに割り当てる必要があります。

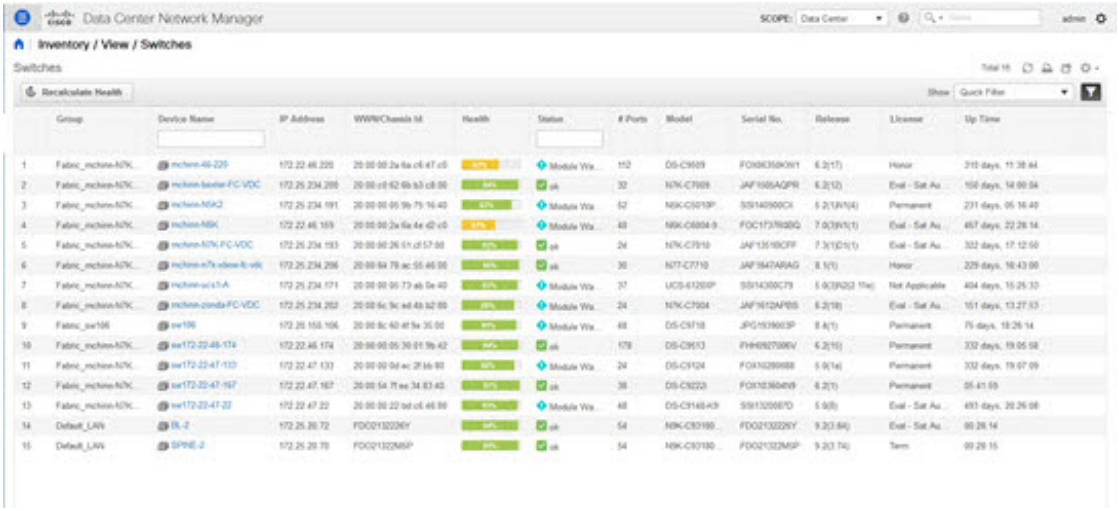
次の図は、オナー モードの SAN スイッチのライセンス ページを示しています。



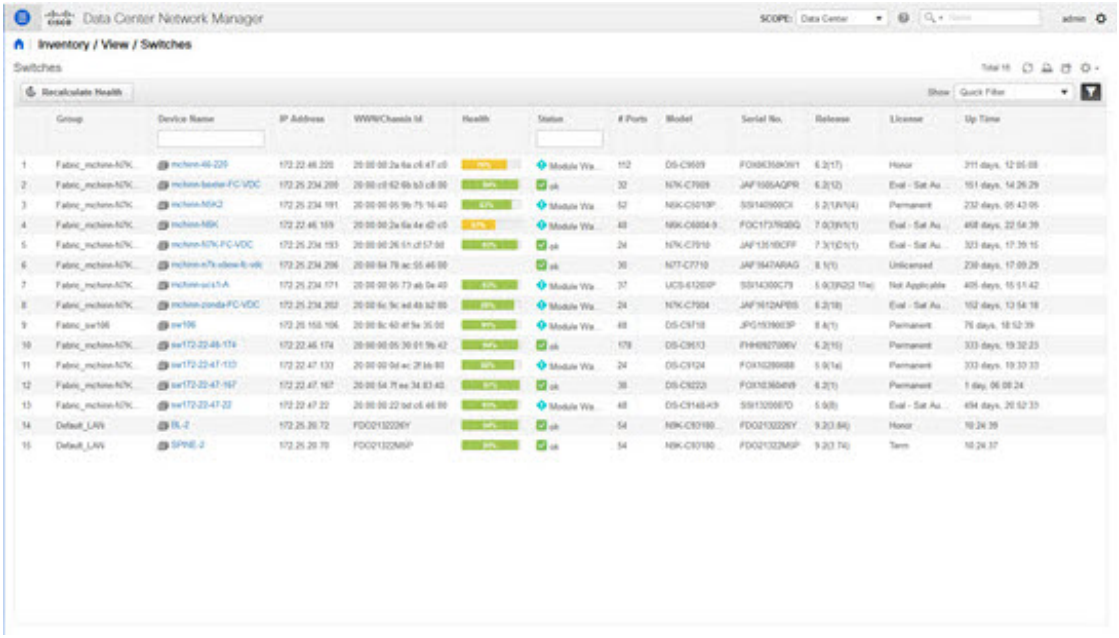
次の図は、オナー モードの LAN スイッチのライセンス ページを示しています。



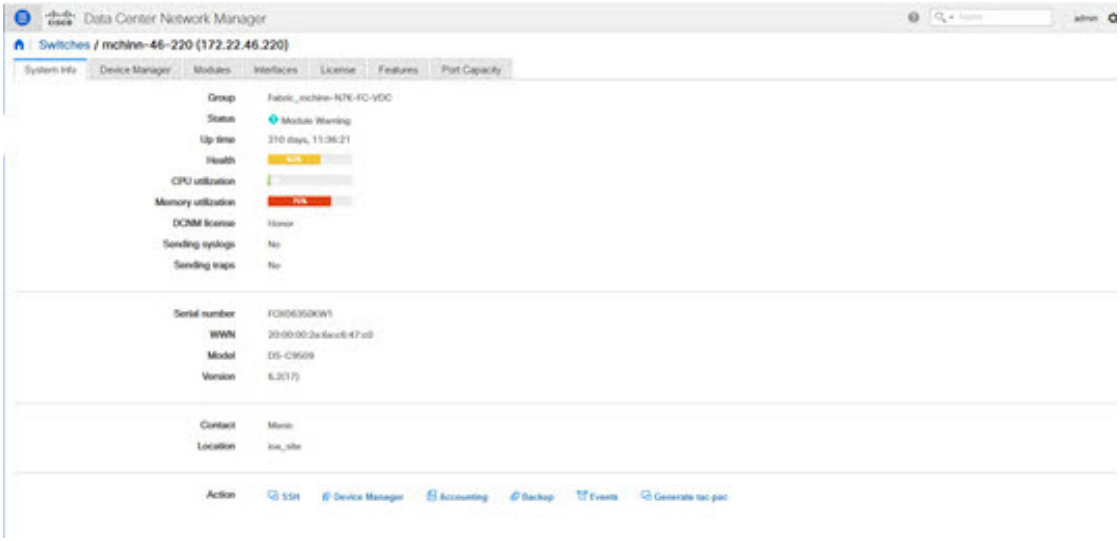
次の図は、ライセンスと期間のオナー モードを表示するスイッチ テーブルを示しています。



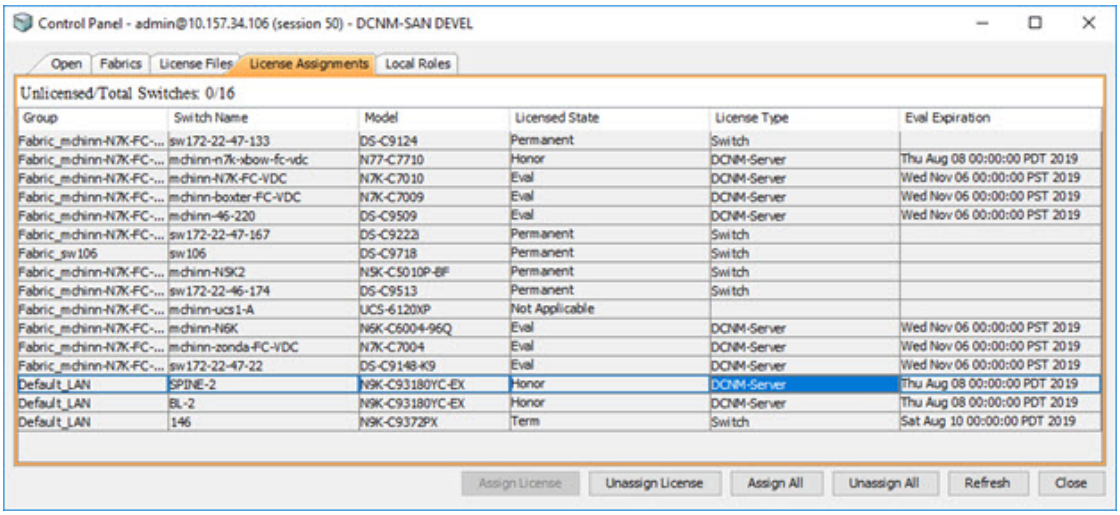
次の画像は、オナー モード ライセンスの LAN スイッチを備えたスイッチ ダッシュボードを示しています。



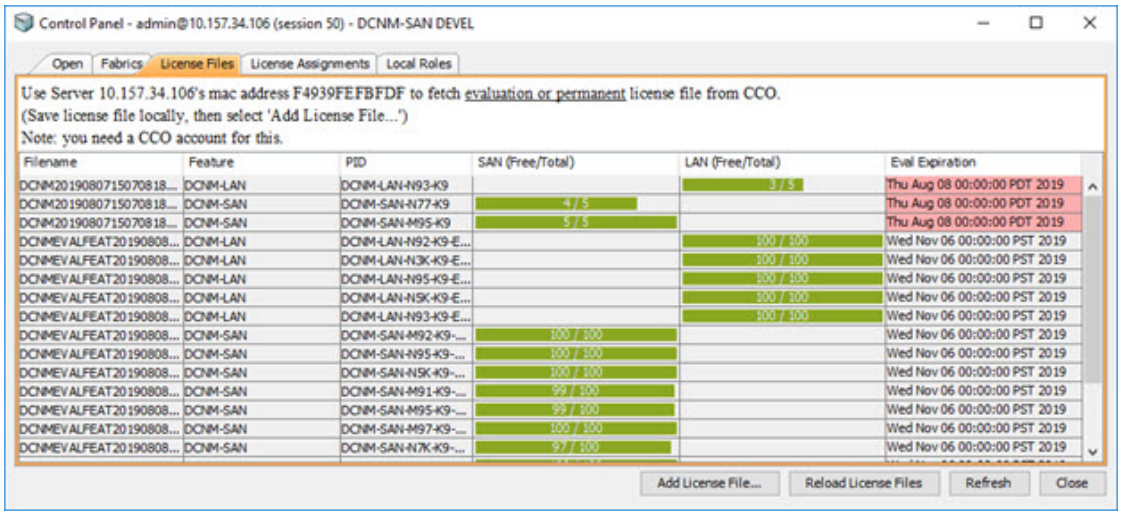
次の図は、オナー モード ライセンスの SAN スイッチを備えたスイッチ ダッシュボードを示しています。



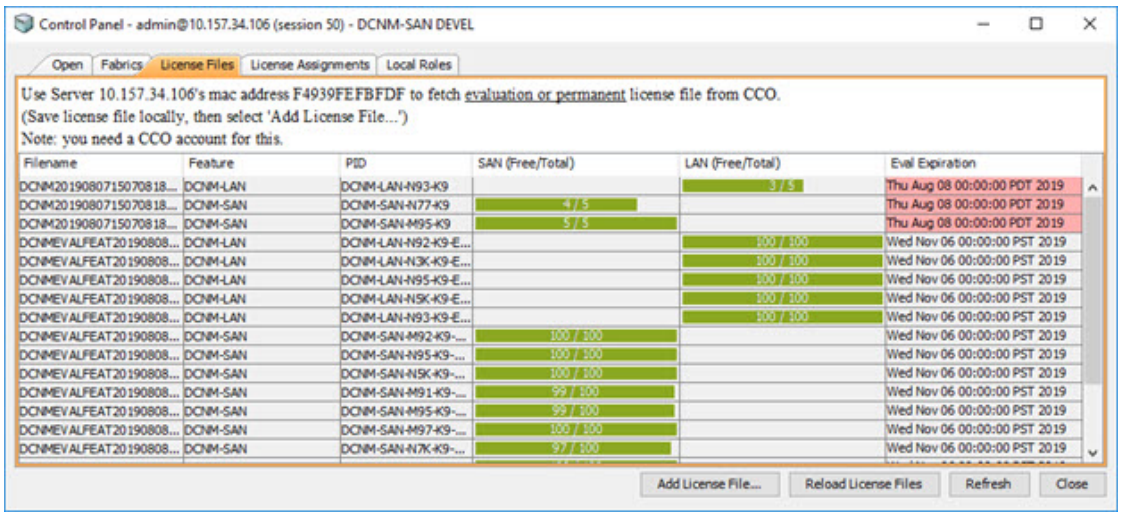
次の図は、SAN クライアント ライセンスの使用許諾契約タブを示しています。



次の図は、**SAN クライアント ライセンス** ファイル タブを示しています。



（注） スイッチベースのオナー ライセンスは、サーバーベースのライセンス ファイルで上書きできません。



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。
- **[制御（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。

フィールド	説明
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。
最終更新日	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 **[制御（Control）]** をクリックし、ドロップダウン リストで **[有効化（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 **[未構成（UNCONFIGURED）]** から **[登録抹消（DEREGISTERED）]** に変わり、ライセンス ステータスが **[未構成（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 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 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 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） 管理モードのスイッチについては、スイッチ スマート ライセンスは DCNM を通して割り当てる必要があります。

（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。
機能	ライセンス機能を指定します。
PID	製品 ID を指定します。
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 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** 構成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。

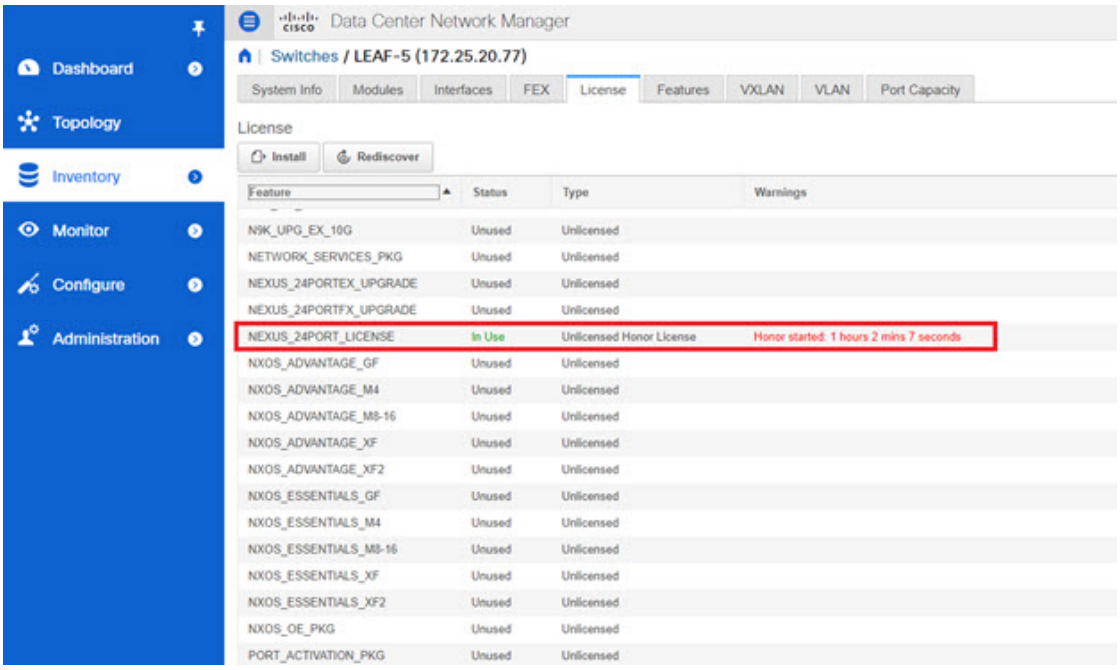
10. **[ライセンスのインストール（Install Licenses）]** をクリックします。

    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。

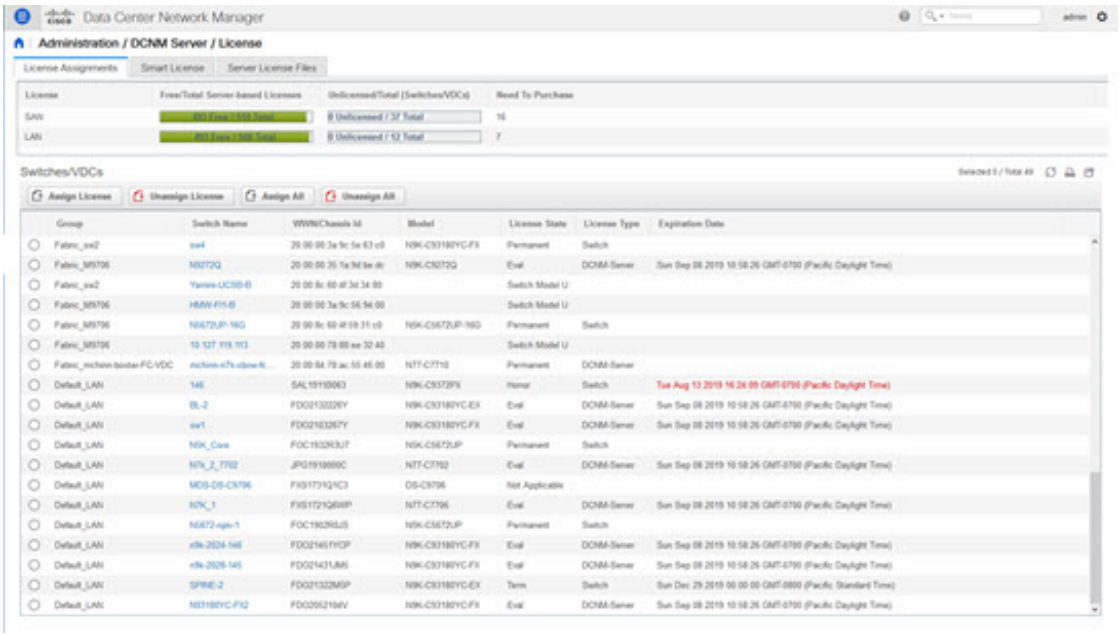
11. ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ライセンスのステータス（License Status）]** テーブルにステータスが表示されます。

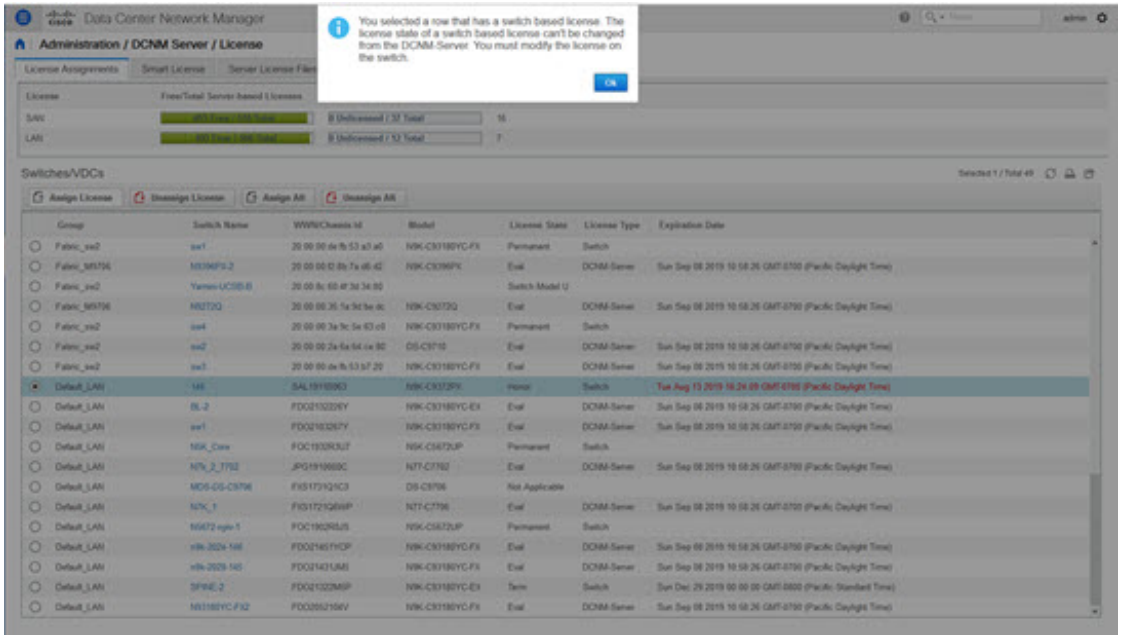
スイッチベースの名誉ライセンスのサポート

[DCNM **Web UI]** > **[インベントリ（Inventory）]** > **[スイッチ（Switch）]** > **[ライセンス（License）]** で、**[タイプ（Type）]** 列に「Unlicensed Honor License」と表示され、**[警告（Warnings）]** 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） スイッチベースのオナー ライセンスは、サーバーベースのライセンス ファイルで上書きできません。

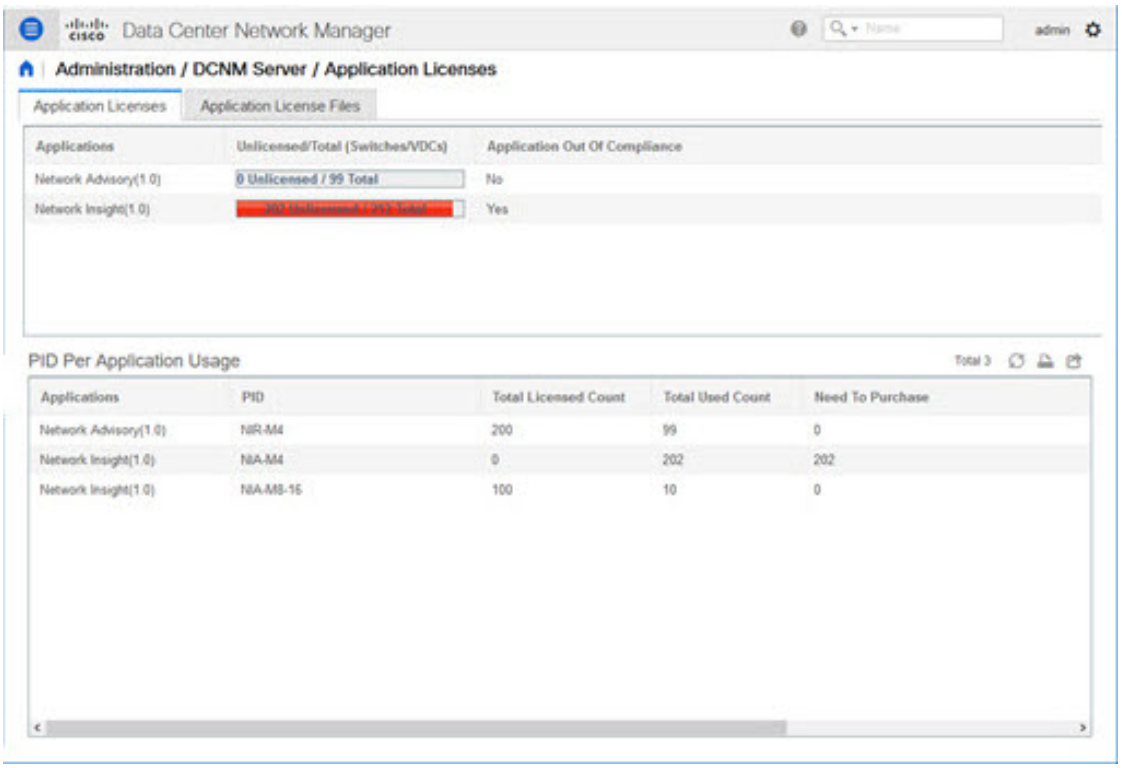




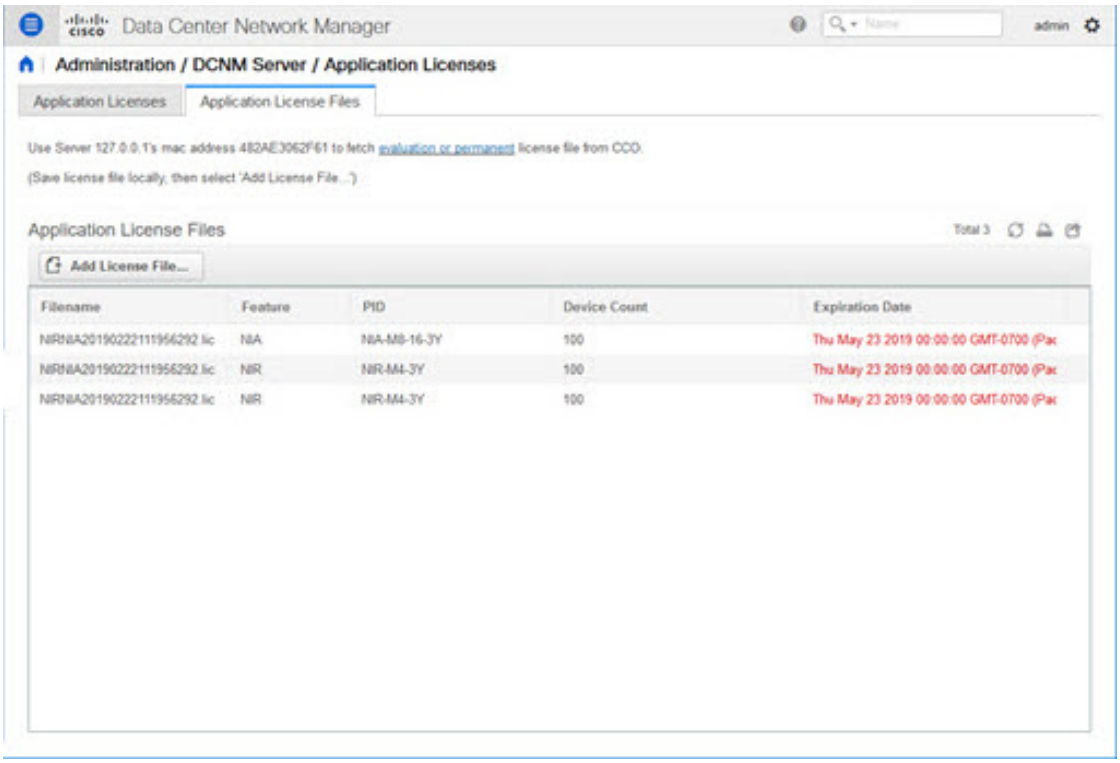
アプリケーション ライセンス

リリース 11.3(1) 以降、Cisco DCNM でアプリケーションのライセンスを管理できます。**[Web UI] > [管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [アプリケーション（Applications）]** を選択して、アプリケーション ライセンスを表示します。

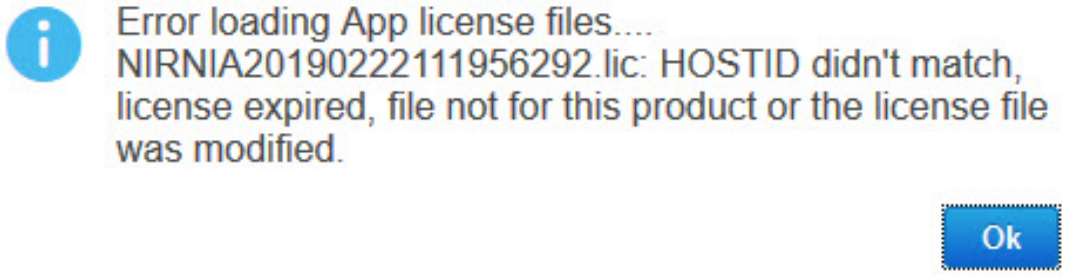
[アプリケーション ライセンス（Application Licenses）] タブには、ライセンスのないスイッチ/合計スイッチの概要、およびコンプライアンスに違反しているかどうかを示す DCNM アプリケーションが表示されます。[アプリケーション使用状況ごとの PID（PID Per Application Usage）] テーブルには、アプリケーション フレームワークからサーバに指定された PID ごとの実際のカウントが表示されます。アプリケーションごとに購入する必要がある PID もリストされています。



[アプリケーション ライセンス ファイル（Application License Files）] タブでは、アプリケーションのライセンス ファイルを追加できます。[ライセンス ファイルの追加（Add license file）] をクリックして、ローカル ディレクトリからライセンス ファイルを追加します。ライセンスのファイル名、アプリケーション名、PID、デバイス数および有効期限日の詳細は、インポートされたライセンス ファイルから抽出されます。ライセンスが永続的でない場合、または評価または期限付きである場合は、有効期限も表示されます。



次の画像は、アプリケーション ライセンス ファイルをアップロードする際のサンプル エラー メッセージを示しています。



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] > [管理ユーザー] > [リモート AAA プロパティ]** 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、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。

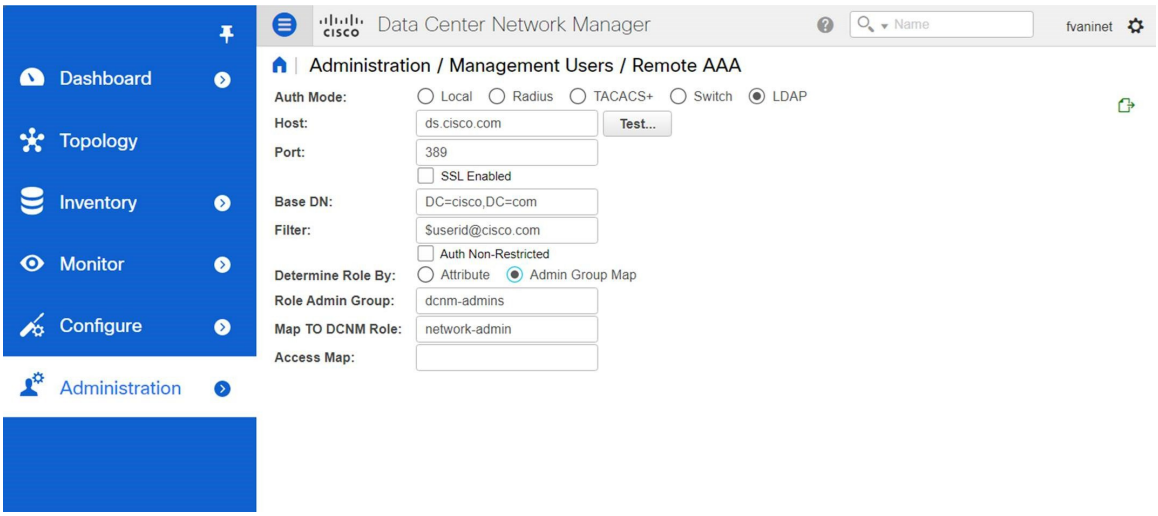
ステップ 3 (Optional) セカンダリおよびターシャリ スイッチの名前を指定します。

ステップ 4 **[適用（Apply）]** をクリックし、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。

DCNM リリース 11.5(1) から、新しいユーザー ロール **device-upg-admin** が追加され、画像管理ウィンドウでのみ操作を実行します。

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]** 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

ローカルユーザー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、ローカルユーザーは、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

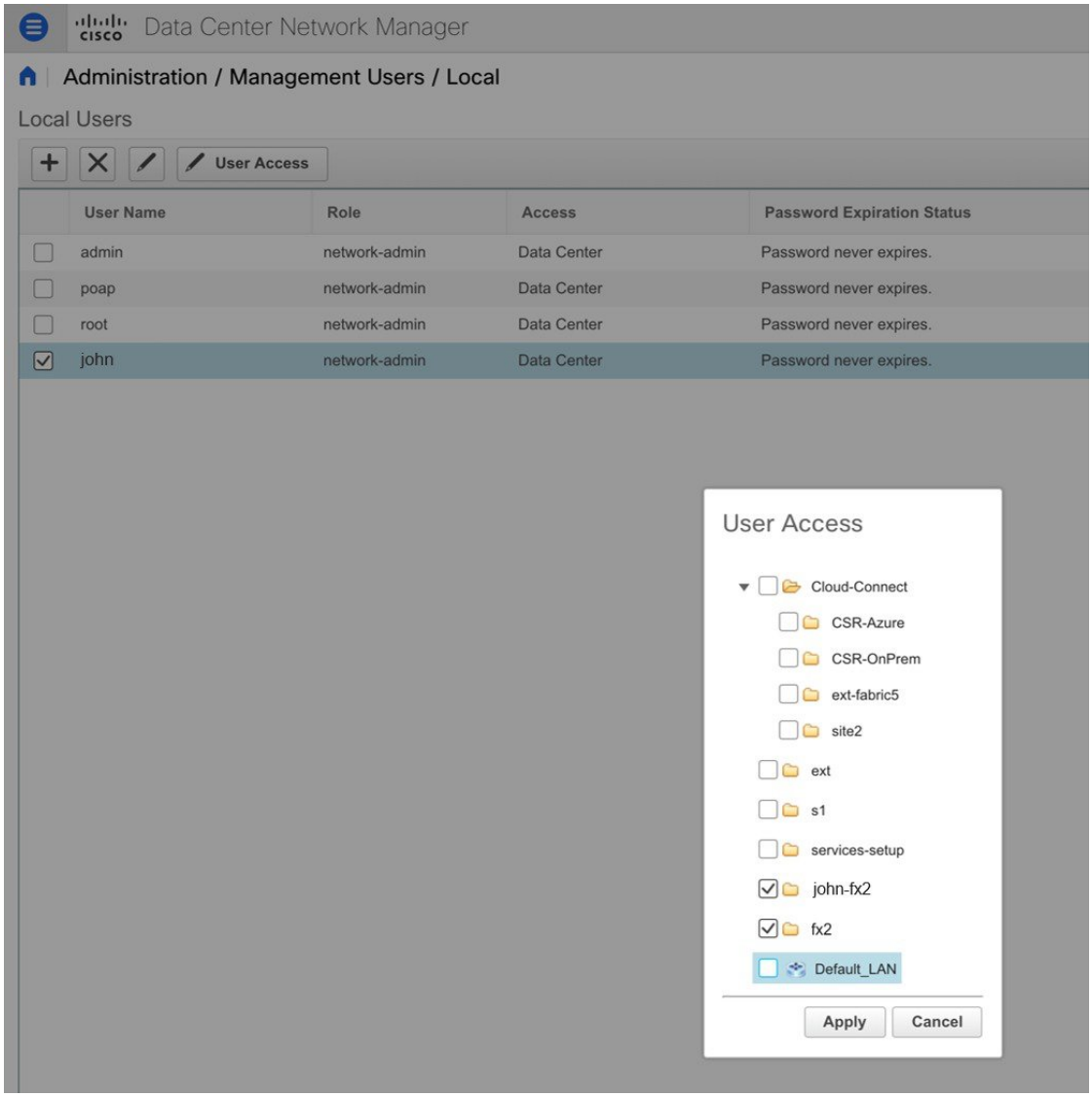
ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザー（Local Users）] ウィンドウが表示されます。

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

[ユーザー 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 ユーザー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。



Note **[ネットワーク管理者（network-admin）]**ロールを持つユーザーにデータ センター全体へのアクセス権がない場合、**[ユーザー アクセス（User Access）]**ボタンはグレー表示され、**[アクセス（Access）]**列の値は**[データ センター（Data Center）]**ではありません。その場合、データセンター全体にアクセスできる新しい**[ネットワーク管理者（network-admin）]**ロールのユーザーを作成するには、*addUser.sh/bat* スクリプトを使用します。

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。

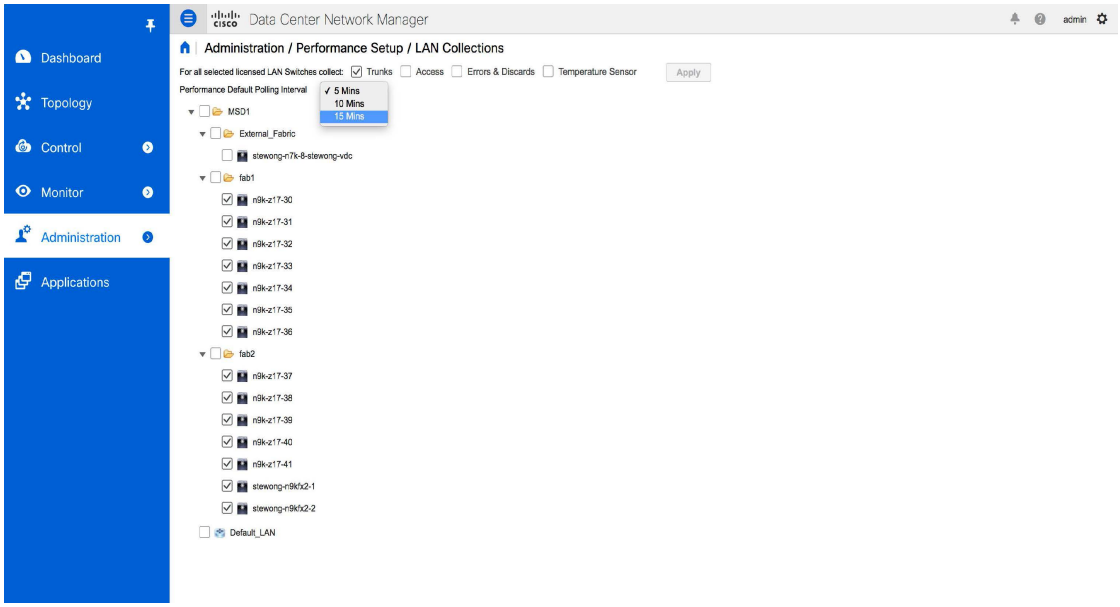
ステップ 2 ライセンスを取得したすべての LAN スイッチについて、チェック ボックスを使用して、**トランク**、**アクセス**、**エラーと破棄**、および**温度センサー**のパフォーマンスデータ収集を有効にします。

ステップ 3 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 4 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 5 [Apply] をクリックして、設定を保存します

ステップ 6 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。



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 で次を構成する必要があります。

- **Syslog の送信**を有効にするには：**[物理的属性（Physical Attributes）]** > **[イベント（Events）]** > **[Syslog]** > **[サーバ（Servers）]** を選択します。**[行の作成（Create Row）]** をクリックし、必要な詳細を入力して、**[作成（Create）]** 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（Create Row）]** をクリックし、必要な詳細を入力して、**[作成（Create）]** をクリックします。
- **遅延トラップ**の有効化：**[物理属性（Physical Attributes）] > [イベント（Events）] > [SNMP トラップ（SNMP Traps）] > [遅延トラップ（Delayed Traps）]** を選択します。**[機能の有効化（Feature Enable）]** 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 レシーバと統計情報が表示されます。

ステップ 2 **[Syslog レシーバを有効にする（Enable Syslog Receiver）]** チェックボックスをオンにして **[適用（Apply）]** をクリックすると、サーバ プロパティで Syslog レシーバ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 のプロパティを構成するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ 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**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（Event Count Filter）]** 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（Snooze）]** チェックボックスを選択して、**[開始（Start）]** 日付と時刻、**[終了（End）]** 日付と時刻を指定します。[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] 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]** 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/ ローカル エリア ネットワーク（LAN）（Fabric/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（Source）]** 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（Minimum Severity）]** 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。

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。**[ローカル エリア ネットワーク（LAN）、ポート グループ（LAN, Port Groups）]** または **[任意（Any）]** を選択できます。**ローカル エリア ネットワーク（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、**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 資格情報管理メニューには、次のサブメニューがあります：

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 つの資格情報のセットを使用して LAN デバイスに接続します。

- **ディスカバリ資格情報**：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**：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。資格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（Switch）] テーブルのデバイスそれぞれに資格情報を指定して、デフォルトの資格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資格情報を入力して **[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資格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、デフォルトの資格情報が使用されます。

スイッチテーブル

[スイッチ（Switch）] テーブルは、ユーザーがアクセスしたすべての 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 64

- 資格情報の検証, on page 64
- スイッチ資格情報のクリア, on page 64
- リモート アクセスによる認証情報管理, on page 65

[DCNM ユーザーの LAN 資格情報（LAN Credentials for the DCNM User）] 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	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、資格情報を編集します。

1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** を選択し、クレデンシャル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。

資格情報の検証

資格情報を検証するには、次のタスクを実行します。

1. **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** から、資格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。

スイッチ資格情報のクリア

次のタスクを実行して、スイッチ資格情報をクリアします。

1. **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]**から、資格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資格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ー 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
- network-stager
- access-admin
- device-upg-admin

各ロールは、特定のカテゴリのリソースに対する読み取りおよびオプションの書き込み権限を許可します。DCNM ロールの詳細については、『Cisco DCNM の拡張されたロールベースのアクセス制御』を参照してください。

デバイス検出ログイン情報と LAN ログイン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 ログイン情報でのみ実行されるため、両者は異なります。デバイス検出ログイン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、これらのログイン情報を使用します。ただし、LAN ログイン情報は、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 にアクセスできる場合、そのユーザーは LAN ログイン情報を入力してデバイスへの書き込みアクセスを取得できます。書き込み操作では、LAN ログイン

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 を構成する場合、ユーザーは次のように LAN ログイン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

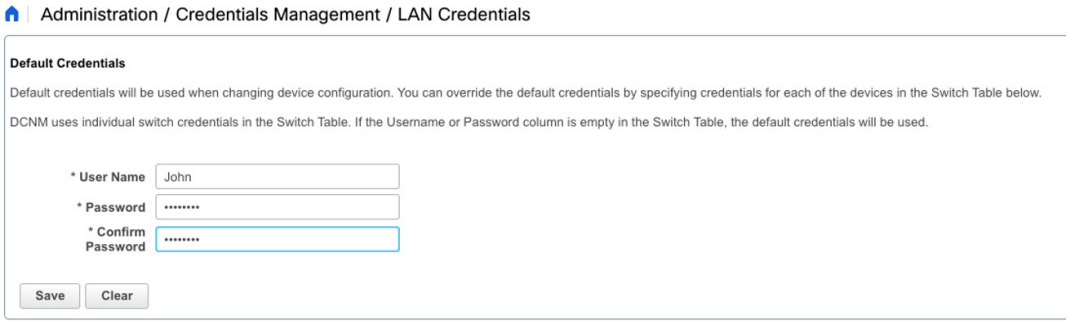
通常の AAA リモート認証

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 ログイン情報の入力を求めます。前述のように、DCNM はこれらのログイン情報を使用して、デバイスへの書き込みアクセスを提供します。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 ログイン情報（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。

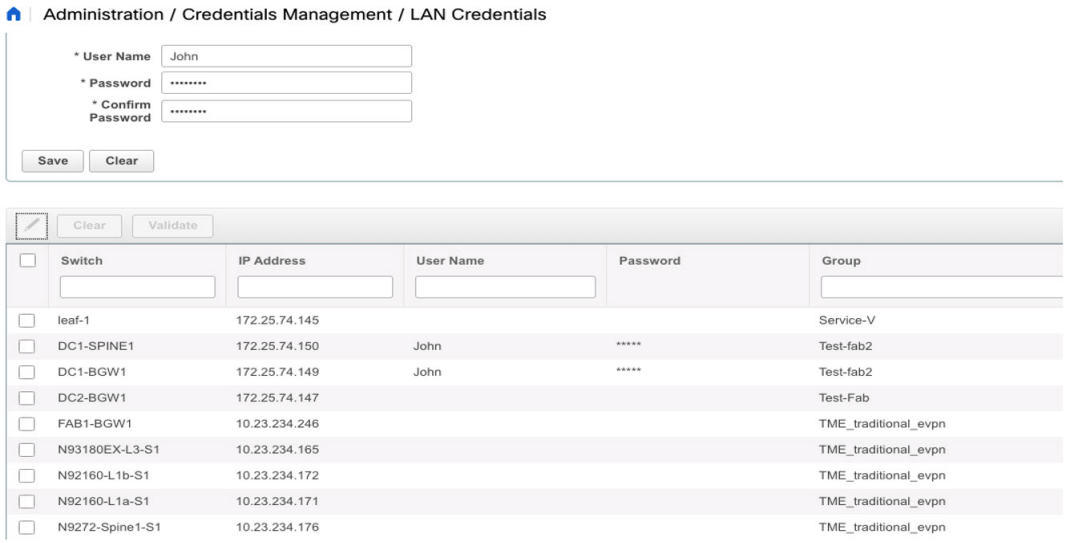
たとえば、ISE サーバーで認証を行う John という名前のユーザーについて考えてみましょう。

1. John は、自分のユーザー ログイン情報を使用して DCNM にログインします。
2. ISE サーバーは John のユーザー ログイン情報を認証し、DCNM は彼の LAN スイッチ ログイン情報を入力するためのメッセージを表示します。DCNM はこれらのログイン情報を使用して、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 スイッチのログイン情報を入力します。DCNM は、すべてのデバイスで John によってトリガーされるすべての書き込み操作に LAN スイッチ ログイン情報を使用します。ただし、ジョンは、デバイスごとのアクセス ベースで LAN スイッチのログイン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、デフォルトのログイン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スイッチログイン情報をすでにキャプチャしているため、LANスイッチログイン情報を入力するためのメッセージを表示しません。Johnは、同じログイン情報を使用して、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 ログイン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 ログイン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 ログイン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 ログイン情報をそのユーザーの LAN スイッチ ログイン情報設定のデフォルトログイン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 ログイン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. **su** コマンドを使用して、/root/ ディレクトリにログインします。
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 ログイン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 ログイン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た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 は更新されたログイン情報をユーザー John に関連付けられたデフォルトの LAN ログイン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。対応するログイン情報を使用して、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 ログイン情報を入力して、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 ログイン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 ログイン情報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 にログインして設定を変更すると、DCNM はロボットの LAN ログイン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、変更をトリガー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に表示します。

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。

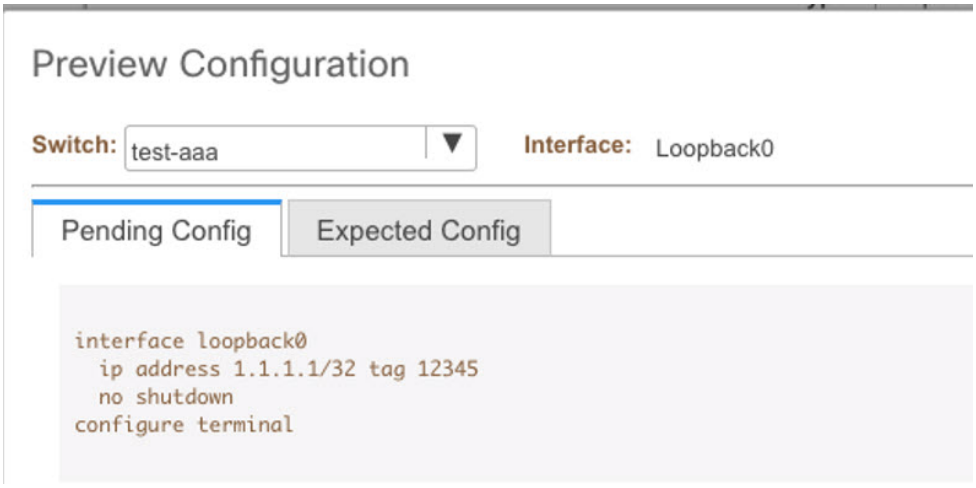
```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

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 ログイン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 ログイン情報（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 ログイン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。

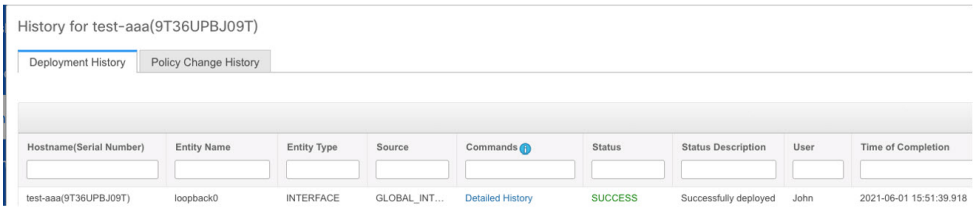
サービス アカウント構成監査

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の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。

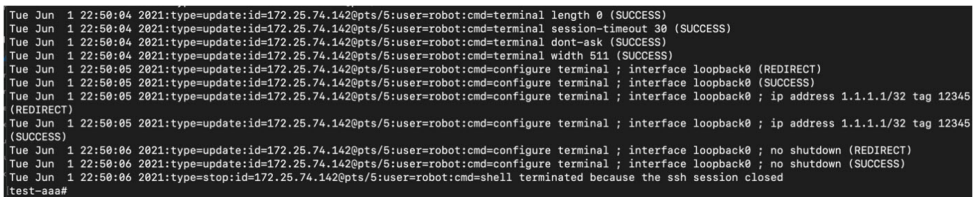
1. John は、デバイスでテスト ループバックを作成します。



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。