NXAPI 証明書

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。証明書は、スイッチ コンソールで CLI コマンドを使用して手動でインストールすること、または Cisco Nexusダッシュボード ファブリック コントローラ を使用してスイッチにインストールすることができます。

Cisco Nexusダッシュボード ファブリック コントローラ では、NX-API 証明書を Nexusダッシュボード ファブリック コントローラ 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、Nexusダッシュボード ファブリック コントローラ 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。

（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。

• 証明書の生成と管理 （1 ページ）

証明書の生成と管理

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 Nexusダッシュボード ファブリック コントローラ 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` ファイルの内容も含めることができます。

Nexusダッシュボード ファブリック コントローラ 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 Nexusダッシュボード ファブリック コントローラは暗号化を義務付けていません。ただし、これは Nexusダッシュボード ファブリック

コントローラ 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。Nexusダッシュボード ファブリック コントローラ は AES 暗号化をサポートしています。

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 Nexusダッシュボード ファブリック コントローラ 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、Nexusダッシュボードファブリック コントローラ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、Nexusダッシュボード ファブリック コントローラ 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、Nexusダッシュボード ファブリック コントローラはスイッチに証明書をインストールできません。

Cisco Nexusダッシュボード ファブリック コントローラ 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） Nexusダッシュボード ファブリック コントローラ 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、Nexusダッシュボード ファブリック コントローラ 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 Nexusダッシュボード ファブリック コントローラ による NX-API 証明書の検証

リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ はスイッチによって提供される NX-API 証明書を検証する機能をサポートしています。Cisco Nexusダッシュボード ファブリック コントローラ が行う NX-API リクエストには SSL 接続が必要です。ス

イッチはSSLサーバーのように動作し、SSLネゴシエーションの一部としてサーバー証明書を提供します。対応する CA 証明書が提供されている場合、Cisco Nexusダッシュボード ファブリック コントローラ はそれを確認できます。

（注） デフォルトでは、NX-API 証明書の検証は有効にされていません。これは、データセンター内のすべてのスイッチに CA 署名付き証明書がインストールされている必要があり、Cisco Nexusダッシュボード ファブリック コントローラ には対応するすべての CA 証明書が供給されるためです。

Cisco Nexusダッシュボード ファブリック コントローラ の NX-API 証明書管理には、同じ対象を管理するためのスイッチ証明書とCA 証明書という 2 つの機能があります。

スイッチ証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切な証明書ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラ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 Nexusダッシュボード ファブリック コントローラ 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。
3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ 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がテーブルに一覧表示されます。

   テーブルには、ステータスが UPLOADED と表示されます。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。

スイッチの割り当てと証明書のインストール

Cisco Nexusダッシュボード ファブリック コントローラ 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。

1. 1 つまたは複数の証明書のチェックボックスをオンにします。

2. **[アクション (Actions)]** ドロップダウンリストから、**[スイッチの割り当てとインストール (Assign Switch & Install)]** を選択します。
3. **[NX API 証明書クレデンシャル (NX API Certificate Credentials)]** フィールドに、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。

   [パスワード (Password)] フィールドは必須ですが、キーがパスワードを使用して暗号化されていない場合は、任意のランダムな文字列を入力できます（たとえばtest、installなど）。暗号化されていないファイルの場合、パスワードは使用されませんが、一括モードであるため、ランダムな文字列を入力する必要があります。

（注） 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ます。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。

4. 証明書ごとに、**[割り当て (Assign)]** の矢印をクリックし、証明書に関連付けるスイッチを選択します。
5. **[証明書のインストール (Install Certificates)]** をクリックして、それぞれのスイッチにすべての証明書をインストールします。

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、Nexusダッシュボードファブリック コントローラはNexusダッシュボードファブリック コントローラ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、Nexusダッシュボードファブリック コントローラ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 Nexusダッシュボード ファブリック コントローラ はスイッチの証明書を削除できません。

Nexusダッシュボード ファブリック コントローラ リポジトリから証明書を削除するには、次の手順を実行します。

1. 削除する必要がある証明書を選択します。
2. **[アクション (Actions)]** ドロップダウン リストから、**[リンク解除 (Unlink)]** を選択します

   確認メッセージが表示されます。
3. **[OK]** をクリックして、選択した証明書をスイッチからリンク解除します。

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。

4. [Switch] から、現在リンク解除されている証明書を選択します。
5. **[アクション (Actions)]** ドロップダウン リストから、**[削除 (Delete)]** を選択します。

   証明書は Nexusダッシュボード ファブリック コントローラ から削除されます。

CA 証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** 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。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラにアップロードする証明書とキーのペアを選択します。

   ファイル拡張子が `.cer/.crt/.pem` ファイル拡張子をもつ証明書を個別に選択できます。

（注） CA 証明書は公開証明書であり、キーは含まれません。また、この操作にはキーは必要ありません。これは、スイッチが提供するNX-API証明書を確認するためにCisco Nexusダッシュボードファブリック コントローラが必要とする証明書です。つまり、CA 証明書はCisco Nexusダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ 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がテーブルに一覧表示されます。

スイッチの割り当てと証明書のインストール

これらのCA 証明書は Cisco Nexusダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

証明書のリンク解除と削除

CA 証明書はスイッチにインストールされないため、リンク解除する必要はありません。

CA 証明書は、特定の CA に新しい証明書を持ち込む必要があるため、削除できます。

[アクション (Actions)] ドロップダウン リストから、**[削除 (Delete)]** を選択します。証明書はNexusダッシュボード ファブリック コントローラ から削除されます。

NX-API 証明書検証の有効化

NX-API 証明書の検証は、[CA 証明書] ページのトグル ボタンを使用して有効にできます。ただし、これは、Cisco Nexusダッシュボード ファブリック コントローラ が管理するすべてのスイッチに CA 署名付き証明書がインストールされ、対応する CA ルート証明書（1つ以上）がCisco Nexusダッシュボード ファブリック コントローラ にアップロードされた後にのみ行う必要があります。これを有効にすると、Cisco Nexusダッシュボード ファブリック コントローラSSLクライアントはスイッチによって提供される証明書の検証を開始します。検証に失敗すると、NX-API コールも失敗します。

（注）

- NX-API 証明書の検証は、スイッチごとに適用できません。 all または none のいずれかです。したがって、すべてのスイッチに対応する CA 署名付き証明書がインストールされている場合にのみ、検証を有効にすることが重要です。
- また、すべての CA 証明書が Cisco Nexusダッシュボード ファブリック コントローラ にインストールされている必要があります。
- 検証の問題が原因で特定のスイッチでNX-API コールが失敗した場合は、トグル ボタンを使用して適用を無効にできます。すべての結果は、以前の状態に戻ります。
- 上記の点から、メンテナンス期間中に適用を有効にする必要があります。