Cisco DCNM サーバのセキュアなクライアント通信

Cisco DCNM サーバのセキュアなクライアント通信

この項では、Cisco Data Center Network Manager Servers で HTTPS を使用する方法について説明します。

Note CA 署名済み SSL 証明書を追加する前に、Cisco DCNM で SSL/HTTPS を有効にする必要があります。したがって、下に記載されている順番で手順を実行します。

この項では、次のトピックについて取り上げます。

仮想アプライアンスの HA 環境で Cisco DCNM 上の SSL/HTTPS を有効にする

HA モードの Cisco DCNM の仮想アプライアンスで SSL/HTTPS を有効にするには、次のことを実行します。

Procedure

ステップ 1 自己署名 SSL 証明書を使用してプライマリ サーバを設定します。

Note CA 署名付き証明書では、各サーバに独自の証明書が生成されます。証明書が両方のサーバで共通の署名証明書チェーンによって署名されていることを確認します。

ステップ 2 セカンダリ サーバでキーストアを検索します。

ステップ 3 次の場所にあるキーストアの名前を変更します

```
< DCNM_install_root
>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks

～

< DCNM_install_root
>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old
```

ステップ 4 プライマリ サーバからセカンダリ サーバに生成された `fmserver.jks` ファイルを、フォルダにコピーします。

```
<dcnm-home> /dcm/wildfly-10.1.0.Final/standalone/configuration/
<dcnm-home>/dcm/fm/conf/cert/
```

What to do next

自己署名付き証明書を作成した場合、SSL 証明書をキーストアにインポートした場合、`/usr/local/cisco/dcm/wildfly-10.1.0.Final/standalone/configuration` にある新しい fmserver.jks を `/etc/elasticsearch` にコピーする必要があります。fmserver.jks ファイルを elasticsearch ディレクトリにコピーしない場合、アラームとポリシーを取得できません。elasticsearch データベースを安定化させるため、Cisco DCNM **[Web UI モニタ (Web UI Monitor)] > [アラーム (Alarms)] > [アラーム ポリシー (Alarm Policies)]** でアラーム ポリシーを設定できません。