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。

このセクションは、次のトピックで構成されています。

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。

このセクションは、次のトピックで構成されています。

RHELまたはWindows上のフェデレーションのCisco DCNMでSSL/HTTPSを有効化する

フェデレーションの Cisco DCNM 向け RHEL または Windows 上で SSL/HTTPS を有効にするには、次の手順を実行します。

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、次のいずれかを実行します。

- インストーラの実行中に、[HTTPS] を選択して、HTTP モードで実行することを選択します。
- サイレント インストールしている間、インストーラの実行中に [HTTPs] を選択します。

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。