SSL 証明書の作成とインストール

(Stealthwatch システム バージョン 6.10 用)

著作権および商標

注意事項

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。このソフトウェアライセンスまたは限定保証を見つけられない場合は、シスコの代理店に連絡しコピーを入手してください。

シスコが導入するTCP ヘッダー圧縮は、カリフォルニア大学バークレー校(UCB)により、UNIX オペレーティングシステムのUCB パブリックドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用しているIP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社のWeb サイト(www.cisco.com/go/offices/) をご覧ください。

目次

1

はじめに

このドキュメントでは、サードパーティまたは内部で検証された証明書を作成し、Stealthwatch システムにインストールする手順を説明します。

(注) Stealthwatch システムでは、PEM 形式の証明書および RSA で暗号化された証明書のみをサポートします。

対象読者

このガイドの主な対象者には、Stealthwatch システムの設定を担当する管理者が含まれています。

はじめる前に

証明書を作成およびインストールする前に、次の手順を実行する必要があります。

- 次の手順に従って、Stealthwatch システムが通信していることを確認します。
- SMC クライアント インターフェイスに移動します。アラーム テーブルを確認し、アクティブな [管理チャネルダウン(Management Channel Down)] アラームまたは [フェールオーバーチャネルダウン(Failover Channel Down)] アラームがないことを確認します。
- SMC クライアント インターフェイスに移動します。[Flow Collectorダッシュボード (Flow Collector Dashboard)] を開きます。ダッシュボードの 3 つのセクションすべてにデータが入力されていることを確認します。
- 適切な Stealthwatch ライセンスがあることを確認します。

(注) 詳細については、*Stealthwatch 証明書のトラブルシューティングガイド*を参照してください。

2

証明書の作成

秘密キーの作成

各アプライアンス(Stealthwatch Management Console、Flow Sensor、Flow Collector、UDP Director) の秘密キーを作成するには、次の手順を実行します。

1. アプライアンスの端末エミュレータウィンドウにアクセスし、アプライアンスの IP アドレスを入力します。
2. root ユーザとしてログインします。
3. 一時フォルダに移動するには、次のコマンドを入力します。

   ```
   cd /lancope/var/admin/tmp
   ```

4. 秘密キーを生成するには、次のコマンドを入力します。

   ```
   openssl genrsa -des3 -out server.key 4096
   ```

5. パスワードを入力して、**Enter** を押します。

   (注) 複数の文字クラスが含まれていて長いけれども覚えておくことができる(少なくとも 2 回入力する必要があります) フレーズを入力します。パスワードのガイドラインについては、米国標準技術局のデジタルアイデンティティガイドラインを参照してください。

6. 秘密キーを復号するには、次のコマンドを入力します。

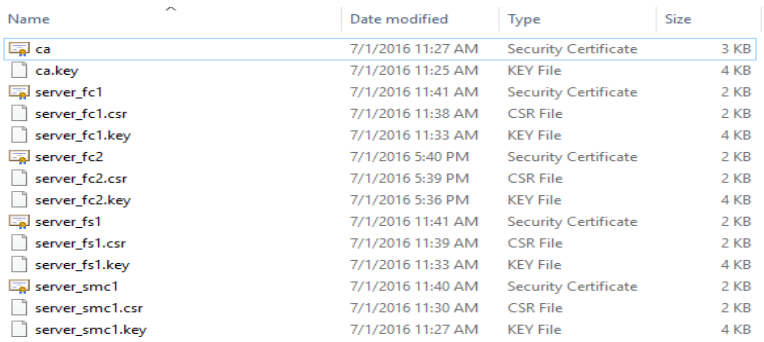
   ```
   cp server.key server.key.org
   openssl rsa -in server.key.org -out server_smc1.key
   ```

   (注) キーは次のリンクからダウンロードできます: https://SMC_IP/smc/files/admin/tmp。また、次の項の手順 6 の後、認証局から証明書が返却された後に復号することもできます。

証明書署名要求の作成

各アプライアンスに対して OpenSSL を使用して証明書署名要求(CSR) を生成するには、次の手順を実行します。

(注) この項を完了すると、複数のサーバ証明書が生成されます。次の図は、作成された証明書の例を示しています。



Name	Date modified	Type	Size
ca	7/1/2016 11:27 AM	Security Certificate	3 KB
ca.key	7/1/2016 11:25 AM	KEY File	4 KB
server_fc1	7/1/2016 11:41 AM	Security Certificate	2 KB
server_fc1.csr	7/1/2016 11:38 AM	CSR File	2 KB
server_fc1.key	7/1/2016 11:33 AM	KEY File	4 KB
server_fc2	7/1/2016 5:40 PM	Security Certificate	2 KB
server_fc2.csr	7/1/2016 5:39 PM	CSR File	2 KB
server_fc2.key	7/1/2016 5:36 PM	KEY File	4 KB
server_fs1	7/1/2016 11:41 AM	Security Certificate	2 KB
server_fs1.csr	7/1/2016 11:39 AM	CSR File	2 KB
server_fs1.key	7/1/2016 11:33 AM	KEY File	4 KB
server_smc1	7/1/2016 11:40 AM	Security Certificate	2 KB
server_smc1.csr	7/1/2016 11:30 AM	CSR File	2 KB
server_smc1.key	7/1/2016 11:27 AM	KEY File	4 KB

1. アプライアンスの端末エミュレータウィンドウにアクセスし、アプライアンスの IP アドレスを入力します。
2. root ユーザとしてログインします。
3. 一時フォルダに移動するには、次のコマンドを入力します。

   ```
   cd /lancope/var/admin/tmp
   ```

4. CSR を生成するには、次のコマンドを入力します。

   ```
   openssl req -new -key server_smc1.key -out server_smc1.csr
   ```

5. 必要な情報を次のように入力します(太字はサンプルの回答) 。詳細については、*Stealthwatch 証明書のトラブルシューティングガイド*を参照してください。

   国名 (2 文字コード) [GB]: **US**

   州/都道府県名 (正式名) [Berkshire]: **Georgia**

   市区町村名 (市など) [Newbury]: **Atlanta**

   組織名 (会社など) [My Company Ltd]: **Your Company Inc**

   組織単位名 (部門など) []: **Information Technology**

   共通名 (名前またはサーバのホスト名など) []: **server_mysmc1.company.com**

   電子メールアドレス []: **john.doe@email.com**

   証明書要求と一緒に送信する以下の「追加の」属性を入力してください。

   チャレンジ パスワード []:

   任意の会社名 []:

注意! 証明書に重複した名前をつけることはできません。共通名は一意である必要があります。完全修飾ドメイン名を使用することをお勧めします。

6. CSR(`server_smc1.csr`) を認証局 (VeriSign または GoDaddy など) または内部 CA に送信し、エンドポイント証明書を作成します。
   a. エンドポイント証明書を作成する場合は、TLS 拡張値および PEM 形式で提供するよう認証局に要求します。
      i. TLS Web サーバ認証 (1.3.6.1.5.5.7.3.1)
      ii. TLS Web クライアント認証 (1.3.6.1.5.5.7.3.2)
   b. CA の指示に従います。

証明書チェーンの作成

サードパーティ証明書から証明書チェーンを作成するには、次の手順を実行します。

(注) SSL エンドポイント証明書をアップロードする場合は、チェーン全体が必要になります。証明書パスが逆になり、ルート CA が最後になります。次に、チェーンの例を示します。

```
Intermediate certificate
--Begin---
<chain>
--End-----

Secondary CA Certificate
--Begin---
<chain>
--End-----

Root CA
--Begin---
<chain>
--End-----
```

1. サードパーティから受信した証明書 zip ファイルを解凍します。
2. 次の手順に従って、Windows に証明書をエクスポートします。

   (注) Mac OS/X ではなくWindows VM を使用して証明書をエクスポートすることをお勧めします。

   a. オペレーティングシステムの証明書ビューアで証明書を開きます。
   b. [証明のパス(Certification Path)] をクリックします。発行元 CA/セカンダリCA/中間 CA を選択し、[証明書の表示(View Certificate)] をクリックします。
   c. 証明書が新しいウィンドウでポップアップされます。[詳細(Details)] をクリックして、[ファイルにコピー(Copy To File)] をクリックします。
   d. エクスポート タイプとして X.509 を使用して、エクスポート ウィザードを実行します。

   (注) ルート CA を含め、証明書のパスの各手順にこれを実行する必要があります。パスの最後の手順で、[証明書の表示(View Certificate)] はグレー表示されます。

3. テキスト エディタを使用して、前述の例のようにチェーン証明書を作成します。

3

証明書のインストール

証明書をインストールするには、次の手順を実行します。

注意！ Stealthwatch アプライアンス間の通信が中断されるため、この手順はメンテナンス ウィンドウで実行することをお勧めします。すべての手順を完了するまで、通信は復元されません。

1. 次の手順を実行して、以前エクスポートしたルート証明局(CA)の証明書とエンドポイント証明書をチェーンを含め各アプライアンスにインストールします。
   a. 証明書を適用するアプライアンスのアプライアンス管理インターフェイスに、管理者ユーザとしてログインします。
   b. メイン メニューから、[設定(Configuration)] > [認証局証明書(Certificate Authority Certificates)] の順に選択します。
   c. [ファイルの選択(Choose File)] または [参照(Browse)] をクリックして、証明書を選択します。
   d. [名前(Name)] フィールドに、証明書を識別する名前を入力します。

   (注) 推奨される名前は、証明書をインストールするアプライアンスのホスト名です。英数字、ダッシュ(-)、アンダースコア(_)、およびドット(.)を使用できます。スペースやその他の特殊文字は使用しないでください。

   e. [証明書の追加(Add Certificate)] をクリックします。
   f. [送信(Submit)] をクリックします。
2. 次の手順に従って、個々のセキュア ソケット レイヤ(SSL)サーバ証明書とキーを各アプライアンスにインストールします。
   a. SSL 証明書を適用するアプライアンのアプライアンス管理インターフェイスに、管理者ユーザとしてログインします。
   b. メイン メニューから、[設定(Configuration)] > [SSL 証明書(SSL Certificate)] を選択します。
   c. [SSLサーバアイデンティティ(SSL Server Identity)] セクションの [ターゲット証明書ファイル(PEMエンコード)(Target Certificate File (PEM-encoded))] フィールドで、[ファイルの選択(Choose File))] または [参照(Browse)] をクリックして、アプライアンスのエンドポイント証明書を含むファイルにアクセスします。
   d. [証明書チェーン(PEMエンコード)(オプション)(Certificate Chain (PEM-encoded) (Optional))] フィールドで、前の章の最後の項で作成したチェーンを追加します。

   (注) 証明書チェーンは、自己署名証明書を使用する場合のみのオプションです。

   e. [秘密キー(非暗号化)(PEMエンコード)(Private Key (Not Encrypted) (PEM-encoded))] フィールドで、[ファイルの選択(Choose File)] または [参照(Browse)] をクリックして、アプライアンスの秘密キー ファイルの場所(`server_smc1.key`)にアクセスします。

f. [証明書のアップロード(Upload Certificate)] をクリックして、入力したフィールドからアプライアンスに証明書をアップロードして適用します。

3. アプライアンスを再起動します。
4. 次の手順に従って、SMC クライアント インターフェイスを使用しているすべてのコンピュータで Java Runtime Environment(JRE) の cacerts ファイルにエンドポイント証明書をインポートします。
   a. 管理者としてコマンド プロンプトを開きます。
   b. ディレクトリを Java Home Bin フォルダに変更します。

> **(注)** 使用している Java のバージョンにエンドポイント証明書をインストールします。パスは、次の例とは異なる場合があります。

   i. Windows のパスの例 :

```
cd C:\Program Files (x86)\Java\jre1.8.0_101\bin
```

   ii. Mac OS/X のパスの例 :

```
cd \System\Library\Internet Plug Ins\JavaAppletPlugin.plugin\Home\bin
```

   c. 次のコマンドを入力して、信頼ストアにエンドポイント証明書をインポートします。
      i. Windows でのコマンド :

```
.\keytool -import -alias <alias> -keystore ..\lib\security\cacerts -file
<path to cert>
```

      ii. Mac OS/X でのコマンド :

```
sudo keytool -import -alias <alias> -keystore ..\lib\security\cacerts -
file <path to cert>
```

   d. キーストア パスワードを入力します。

> **(注)** デフォルトのキーストア パスワードは changeit です。

   e.「 **yes**」と入力して、証明書を信頼します。
5. Stealthwatch に接続するすべてのコンピュータのオペレーティング システム証明書ストア/キーチェーンにエンドポイント証明書をインストールします。オペレーティング システムのヘルプを参照してください。

4

検証

証明書が適切に機能していることを確認するには、次の手順を実行します。

(注) この項はオプションですが、強く推奨されます。

1. SMC Web アプリケーションにログインします。ブラウザの南京錠アイコンをクリックして、証明書を表示します。デフォルトの Lancope 証明書ではなくエンドポイント証明書を使用していることを確認します。
2. SMC クライアント インターフェイスに移動します。アラーム テーブルを確認し、アクティブな [管理チャネルダウン(Management Channel Down)] アラームまたは [フェールオーバーチャネルダウン(Failover Channel Down)] アラームがないことを確認します。
3. SMC クライアント インターフェイスに移動します。[Flow Collectorダッシュボード (Flow Collector Dashboard)] を開きます。ダッシュボードの 3 つのセクションすべてにデータが入力されていることを確認します。データがない場合は、証明書の設定に問題がある可能性があります。次の図は、ダッシュボードの例を示しています。