SMAで証明書を生成してインストールする方法

内容

[概要](#)
[前提条件](#)
[SMAで証明書を生成してインストールする方法](#)
[ESAからの証明書の作成とエクスポート](#)
[エクスポートされた証明書の変換](#)
[OpenSSLを使用した証明書の作成](#)
[追加オプション、ESAからの証明書のエクスポート](#)
[SMAへの証明書のインストール](#)
[例](#)
[SMAでインポートおよび設定された証明書を確認する](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Security Management Appliance(SMA)の設定と使用のために証明書を生成してインストールする方法について説明します。

前提条件

openssl**コマンドをローカルで実行するには、アクセス権が必要になります。**

Eメールセキュリティアプライアンス(ESA)への管理者アカウントアクセスと、SMAのCLIへの管理者アクセスが必要です。

次の項目を.pem形式で使用できる必要があります。

- X.509 証明書
- 証明書に一致する秘密キー
- 認証局(CA)によって提供される中間証明書

SMAで証明書を生成してインストールする方法

> **ヒント**：信頼できるCAによって署名された証明書を使用することをお勧めします。特定のCAは推奨されません。 使用するCAに応じて、署名付き証明書、秘密キー、および中間証明書（該当する場合）をさまざまな形式で受信できます。 証明書をインストールする前に、CAに提供するファイルの形式を調査するか、CAと直接話し合ってください。

現在、SMAはローカルでの証明書の生成をサポートしていません。 代わりに、ESAで自己署名証明書を生成できます。これは、SMAの証明書をインポートおよび設定するための回避策として使用できます。

ESAからの証明書の作成とエクスポート

1. ESAのGUIで、[Network] > [Certificates] > [Add Certificate]から自己署名証明書を作成します。 自己署名証明書を作成する際には、証明書を正しく使用できるように、ESAではなくSMAのホスト名を「共通名(CN)」で使用することが重要です。
2. 変更を送信し、保存します。
3. [Network] > [Certificates] > [Export Certificates]から作成した証明書をエクスポートします。 (1)自己署名証明書として**エクスポートおよび保存/使用、または(2)証明書署名要求のダウンロード（外部で証明書を署名する必要がある場合）の2つのオプションがあります。 自己署名証明書として保存/使用： [証明書のエクスポート]を選択します**証明書を変換するときに使用するファイル名（mycert.pfxなど）とパスフレーズを入力します。これにより、ファイルをローカルに保存するように自動的に求められます。「エクスポートされた証明書の変換」に進みます。証明書署名要求のダウンロード **[Network] > [Certificates] に移動します。**作成した証明書名をクリックします。[署名の発行元]セクションで、[証明書の署名**要求のダウンロード]をクリックします。**.pemファイルをローカルに保存し、CAに送信します。

エクスポートされた証明書の変換

ESAから作成およびエクスポートされる証明書は.pfx形式になります。SMAはインポート用の.pem形式のみをサポートしているため、この証明書を変換する必要があります。 証明書を.pfx形式から.pem形式に変換するには、次の**openssl**コマンドの例を使用します。

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

ESAから証明書を作成する際に使用するパスフレーズの入力を求められます。 OpenSSLコマンドで作成された.pemファイルには、証明書と.pem形式のキーの両方が含まれます。 これで、SMAで証明書を設定する準備ができました。 この記事の「証明書のインストール」セクションに進んでください。

OpenSSLを使用した証明書の作成

または、PC/ワークステーションから**openssl**を実行するためのローカルアクセス権がある場合は、次のコマンドを発行して証明書を生成し、必要な.pemファイルと秘密キーを2つの別のファイルに保存できます。

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout sma_key.pem -out sma_cert.pem
```

これで、SMAで証明書を設定する準備ができました。 この記事の「証明書のインストール」セクションに進んでください。

追加オプション、ESAからの証明書のエクスポート

前述のように、証明書を.pfxから.pemに変換する代わりに、ESAのパスワードをマスキングせずにコンフィギュレーションファイルを保存できます。保存したESA .xml設定ファイルを開き、<certificate>タグを検索します。証明書と秘密キーは既に.pem形式になります。次の「証明書のインストール」セクションで説明されているように、証明書と秘密キーをSMAにインポートするためにコピーします。

注：このオプションは、AsyncOS 11.1以前を実行しているアプライアンスでのみ有効です。このアプライアンスでは、「プレーン・パスフレーズ」オプションを使用して構成ファイルを保存できます。 AsyncOSの新しいバージョンでは、パスフレーズをマスクするか、パスフレーズを暗号化するかのオプションだけが提供されます。 どちらのオプションも秘密キーを暗号化します。これは、証明書のインポートまたは貼り付けのオプションに必要です。

注：上記の「#2の証明書署名要求のダウンロード」を選択し、CAによって証明書が署名されている場合は、証明書と秘密キーのコピーを作成するための設定ファイルを保存する前に、証明書が作成されたESAに署名付き証明書をインポートする必要があります。インポートは、ESA GUIで証明書名をクリックし、[Upload Signed Certificate]オプションを使用して実行できます。

SMAへの証明書のインストール

1つの証明書をすべてのサービスに使用することも、個別の証明書を4つのサービスそれぞれに使用することもできます。

- インバウンド TLS
- アウトバウンド TLS
- HTTPS
- LDAPS

SMAで、CLIを使用してログインし、次の手順を実行します。

1. certconfigを実行します。
2. セットアップオプションを選択します。
3. すべてのサービスで同じ証明書を使用するか、個々のサービスごとに個別の証明書を使用するかを選択する必要があります。「Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and LDAPS?」というメッセージが表示されたら、「Y」と答えると、証明書とキーを一度入力するだけで、その証明書をすべてのサービスに割り当てることができます。「N」を入力する場合、プロンプトが表示されたら、各サービスの証明書、キー、中間証明書（該当する場合）を入力する必要があります。インバウンド、アウトバウンド、HTTPS、および管理
4. プロンプトが表示されたら、証明書またはキーを貼り付けます。
5. 末尾に「。」 現在の項目の貼り付けが完了したことを示すために、エントリごとに独自の行に表示されます。 （「例」セクションを参照）。
6. 中間証明書がある場合は、プロンプトが表示されたら必ず入力してください。
7. 完了したらEnterキーを押し、SMAのメインCLIプロンプトに戻ります。
8. commitを実行して設定を保存します。

注：Ctrl+Cを使用してcertconfigコマンドを終了しないでください。変更はただちにキャンセルされます。

例

```
mysma.local> certconfig

Currently using the demo certificate/key for receiving, delivery, HTTPS management access, and
LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
[]> setup

Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and
LDAPS? [Y]> y

paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAwIJAIXvIlkArow9MA0GCSqGSIb3DQEBBQUAMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzAeFw0xNzExMTAxNjA3MTRaFw0yNzExMDgxNjA3MTRaMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPz0perw3QA
ZH8xctOrvvjsnOPkItmSc+DUqtVKM6OOOkNHA2WY9XJ3+vESwkIdwexibj6VUQ85
K7NE6zOgRfpYdQsxmpIWhzYf9qCBOXuKsRw/9jonKk98DfHFM02J3BSmmgZ0MPp7
6EwA/sZAN+aqYB7IE1fgnqpEXek8xFlfcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqqQHhhJ
pSO7PbevxwanYVXvNR8o2feAWs5LYkrwqdGRxLJmHjFnMV3PbkwRPgFWQ6AD1g12
34==
-----END CERTIFICATE-----
.
paste key in PEM format (end with '.'):
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCj89KXq8N0AGR/
MXLTq7747Jzj5CLZknPg1KrVSjOjjjpDRwNlmPVyd/rxEsJCHcHsYm4+lVEPOSuz
ROszoEX6WHULMZqSFoc2H/aggTl7irEcP/Y6JypPfA3xxTNNidwUppoGdDD6e+hM
AP7GQDfmqmAeyBNX4J6qRF3pPMRZX3FZ0tmE3OzV8+/JTStI71zrQlQa1hbtM5RJ
mVaQI9ACpM9Z7o783zqhM3nfrY2rma+5wyGok684SyrXuKSVJt0+tavz4XoLzSMv
1hzdcaIz/hc40QFJZrZozMx8jNv//3ZqvCYr1JWi11/b1H3St1VYiDiM+M54Bkc/
OUFzu4r3AgMBAAECggEAB9EFjsaZHGwyXmAIpe/PvIVnW3QSd0YEsUjiViXh/V+4
BmIZ1tuqhAkVVS38RfOuPatZrzEmOrASlcro3b6751oVRnHYeTOKwblXZEKU739m
vz6Lai1Y1o5HCepJbl5uuCtTN5CNjzueERWRD/ma0Kv5xi3qwitK1TpKMeb8Q3h2
YABmpk0TyJQ5ixLw3ch9ru1nqiO5zQ91GvIuDckudUu/bBnao+jV7D362lIPyLG8
03GqNviNZ6c3wjD0yQWg619g+ZmjM8DTtDR16zmzBvQ4TgZi22sUWrSSILRa69jW
q8XszQVRydl+gt666iUeN/ozmEMt5J8pu3i9vf3G2QKBgQDHyfv55rjZbWyf0eAT
Ch5T1YsjjMgMOtC9ivi5mMQCunWyRiyZ6qqSBME9Tper/YdAA07PoNtTpVPYyuVX
DDmyuWGHE04baf5QEmSgvQjXOSUPN5TI9hc5/mtvD8QjDO6rebUWxV3NJoR7YNrz
OmfARMXxaF+/mEj+6blSjZuGaQKBgQDSFKvYownPL6qTFhIH7B3kOLwZHk6cJUau
Zoaj7vTw7LrVJv1B0iLPmttEXeJgxzlFYR8tzfn0kTxGQlnhQxXkQ1kdDeqaiLvm
0TtmHMDupjDNKCNH8yBPqB+BIA4cB+/vo23W1HMHpGgqYWRRX/qremL72XFZSRnM
B8nRwK4aXwKBgB+hkwtVxB5ofLIxAFEDYRnUzVqrh2CoTzQzNH3t+dqUut2mzpjv
1mGX7yBNuSW51hgEbg3hYdg0bLn+JaFKhjgNsas5Gzyr41+6CcSJKUUp/vwRyLSo
gbTk2w2SaXNDMOZlNo6MYPWCC6edBg1MSfDe8pft9nrXGXeCeZzgXqdBAoGAQ6Iq
DQ24O76h0Ma7OVe36+CkFgYe0sBheAZD9IUa0HG2WKc7w7QORv4Y93KuTe/1rTNu
YUW94hHb8Natrwr1Ak74YpU3YVcB/3Z/BAnfxzUz4ui4KxLH5T1AH0cdo8KeaW0Z
EJ/HBL/WVUaTkGsw/YHiWiiQCGmzZ29edyvsIUsCgYEAvJtx0ZBAJ443WeHajZWm
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ5l
```

```
k6o79mYhfrTMa4LlHOTyScvuxELqow82vdj6gqX0HVj4fUyrrZ28MiYOMcPw6Y12
34VjKaAsxgZIgN3LvoP7aXo=
-----END PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n

Currently using one certificate/key for receiving, delivery, HTTPS management access, and LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
- PRINT - Display configured certificates/keys.
- CLEAR - Clear configured certificates/keys.
[]>

mysma.local> commit

Please enter some comments describing your changes:
[]> Certificate installation

Changes committed: Fri Nov 10 11:46:07 2017 EST
```

SMAでインポートおよび設定された証明書を確認する

1. HTTPS(https://<SMA IPまたはホスト名>)を使用してGUI経由でSMAに接続し、ログイン資格情報を入力します。
2. ブラウザのアドレスバーのURLの横にあるロックアイコンまたは情報アイコンをクリックして、証明書、有効期限などの有効性を確認します。 使用しているブラウザによって、操作と結果は異なります。
3. 証明書のチェーンを確認するには、[Certification Path]をクリックします。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems