SMA で証明書を生成しインストールする方法

目次

概要

この文書に Ciscoセキュリティ管理機器（SMA）で設定および使用のための証明書を生成しインストールする方法を記述されています。

前提条件

コマンド **openssl** をローカルで実行するアクセスできる必要があります。

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、および SMA の CLI への admin アクセスを必要とします。

.pem 形式で利用可能なこれらの項目を持たなければなりません:

- 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 で証明書を生成しインストールする方法

> **ヒント**：（適当ところ）とはたらかせることを選択する CA によって推奨しません特定の CA.をさまざまなフォーマットの署名入り認証、プライベートキーおよび中間証明書を受け取るかもしれません証明書を信頼された CA. Cisco によって署名してもらうことを推奨します。 CA と直接それらが証明書をインストールする前にあなたに提供するファイルのフォーマットを研究するか、または論議して下さい。

現在、SMA は証明書をローカルで生成することをサポートしません。 その代り、ESA で自己署名証明書を生成することは可能性のあるです。 対応策としてこれが SMA のための証明書をインポートされ、設定されるために作成するのに使用することができます。

ESA からの Export certificate 作成すれば

1. ESA GUI から、**ネットワーク > 証明書 > Add** からの自己署名入り認証を**証明書**作成して下さい。 自己署名証明書を作成するとき、「Common Name （CN）が」とない ESA の… -証明書が正しく使用することができるように SMA …ホスト名を使用することは重要です。
2. 変更を送信し、保存します。
3. 作成される**ネットワーク > 証明書 > Export certificate** から証明書をエクスポートして下さい。 （証明書を外部に署名してもらう必要があれば）自己署名証明書として 2 つのオプションが、（1）エクスポートおよび保存/使用、または（2）ダウンロード証明書署名要求あります: 自己署名証明書として保存/使用: **証明書を**『Export』 を選択 して下さいそれに使用するパスフレーズおよびファイル名を（例えば mycert.pfx）与えて下さい証明書を変換した場合。これは自動的にファイルをローカルで保存するためにプロンプト表示します。エクスポートされた証明書」を変換することを「続行して下さい。証明書署名要求をダウンロードして下さい **ネットワーク > 証明書**作成した証明書名前をクリックして下さい。」セクションによって発行される「シグニチャでは『Download』 をクリック して下さい**証明書署名要求を…**.pem ファイルをローカルで保存し、CA に入れて下さい。

エクスポートされた証明書を変換して下さい

ESA から作成され、エクスポートされた証明書は .pfx フォーマットにあります。 SMA はインポートのための .pem フォーマットだけをサポートします、従ってこの証明書は変換される必要があります。 .pfx フォーマットから .pem フォーマットに証明書を変換するために、次の **openssl** コマンド例を使用して下さい:

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

ESA からの証明書を作成している間使用されたパスフレーズのためにプロンプト表示されます。 openssl コマンドで作成された .pem ファイルは .pem フォーマットで証明書およびキーが両方含まれています。 証明書は SMA で設定されて現在準備ができています。 セクションは「この記事の証明書」インストールするために続行します。

OpenSSL で証明書を作成して下さい

また PC/workstation から **openssl を**実行するローカルアクセスをアクセスできれば証明書を生成し、2 つの個々のファイルに必要な .pem ファイルおよびプライベートキーを保存する次のコマンドを発行できます:

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

証明書は SMA で設定されて現在準備ができています。 セクションは「この記事の証明書」インストールするために続行します。

ESA から証明書をエクスポートする追加オプション

.pem に .pfx からの証明書を、前述のように変換するかわりに、ESA でパスワードを覆わないでコンフィギュレーション ファイルを保存することができます。 <certificate> タグのための保存された ESA .xml コンフィギュレーション ファイルおよび検索を開いて下さい。 証明書およびプライベートキーは .pem フォーマットに既にあります。 「インストール証明書」記述されていると SMA に同じをインポートするための証明書およびプライベートキーを下記の例コピーして下さい

。

注: 上記の #2 を選択した場合「証明書署名要求」をダウンロードし、証明書を CA によって署名してもらって下さい証明書が証明書およびプライベートキーのコピーを撮るためのコンフィギュレーション ファイルを保存する前にから作成された ESA に戻って署名入り認証をインポートする必要があります。 インポートは ESA GUI および使用オプション「アップロード署名入り認証」の証明書名前をクリックしてすることができます。

SMA で証明書をインストールして下さい

単一証明書はすべてのサービスに使用することができますまたは個々の証明書は 4 つのサービスのそれぞれに使用することができます:

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

SMA で、CLI によって ログイン し、次のステップを完了して下さい:

1. **certconfig を**実行して下さい。
2. **セットアップ オプションを**選択して下さい。
3. かどうか同じ証明書をすべてのサービスのために使用するか、または各個々のサービスのために別々の証明書を使用するために選択する必要があります:「示されたとき受信、配達、HTTPS 管理アクセスおよび LDAPS のために 1 つの証明書/キーを使用したいと思うためにか。」、返事「Y は」だけ証明書で入り、一度キー入力するように要求し次にすべてのサービスにその証明書を割り当てます。「N」を入力することを選択する場合プロンプト表示されたとき (適当ところ) 各サービスのための証明書、キーおよび中間証明書で入る必要があります: 受信、送信、HTTPS および管理
4. プロンプト表示された場合、証明書を貼り付けるか、またはキー入力して下さい。
5. と「終了して下さい。「単独で各エントリのための行現在の項目を貼り付けている終了することを示すため。 (セクション「例」参照して下さい。)
6. 中間証明書がある場合、そうするためにプロンプト表示された場合それを入力すること確実でであって下さい。
7. 完了される、SMA の主要な CLI プロンプトに戻るために『Enter』 を押して下さい。
8. 設定を保存するために**託します**実行して下さい。

注: Ctrl+C キーで **certconfig** コマンドを終了しないでください。これは、変更をただちにキャンセルします。

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 のインポートされ、設定された証明書を確認して下さい

1. SMA に GUI で HTTPS を使用して (https:// <SMA IP かホスト名 >) 接続し、ログオン信任状で入力して下さい。
2. ブラウザのアドレスバーの URL の隣で、証明書、終止、等の妥当性をチェックするためにロック アイコンか情報アイコンをクリックして下さい。 どのによってはブラウザを使用しているか、操作および結果は変わるかもしれません。
3. 証明書のチェーンをチェックするために認証パスをクリックして下さい。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems