FMCおよびFDM用のCAバンドルの自動更新の設定

内容

概要

このドキュメントでは、Secure Firewall Management Center(FMC)およびSecure Firewall Device ManagerのCisco CAバンドルの自動更新の使用について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Management Center（旧称Firewall Management Center）およびSecure Firewall Device Manager(旧称Firepower Device Manager)に関するFirepower。
- Secure Firewall Appliance(以前のFirepower)に関する知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン7.0.5以降を実行しているCisco Secure Firewall Management Center（FMC 1000、1600、2500、2600、4500、4600、および仮想）

- ソフトウェアバージョン7.1.0-3以降を実行しているCisco Secure Firewall Management Center（FMC 1600、2600、4600、および仮想）。
- ソフトウェアバージョン7.2.4以降を実行しているCisco Secure Firewall Management Center（FMC 1600、2600、4600、および仮想）。
- ソフトウェアバージョン7.0.5以降を実行し、Secure Firewall Device Managerによって管理されるCisco Secure Firewall（FPR 1000、2100、3100、4100、9300、ISA3000、仮想）。
- ソフトウェアバージョン7.1.0-3以降を実行するCisco Secure Firewall（FPR 1000、2100、3100、4100、9300、ISA3000、および仮想）は、Secure Firewall Device Managerによって管理されます。

- ソフトウェアバージョン7.2.4以降を実行し、Secure Firewall Device Managerによって管理されるCisco Secure Firewall（FPR 1000、2100、3100、4100、9300、ISA3000、および仮想）。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco CAバンドルの用途

Cisco Secure Firewall(旧称Firepower)デバイスは、証明書を含むローカルCAバンドルを使用して、複数のシスコサービス（Smart Licensing、Software、VDB、SRU、およびGeolocation Updates）にアクセスします。システムは、毎日のシステム定義時間に、新しいCA証明書を自動的にシスコに照会します。以前は、CA証明書を更新するためにソフトウェアをアップグレードする必要がありました。

注：この機能は、バージョン7.0.0から7.0.4、7.1.0から7.1.0-2、または7.2.0から7.2.3ではサポートされていません。サポートされているバージョンからサポートされていないバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。

SFMCおよびSFDMでのCAバンドルの自動更新の設定

CAバンドルの自動更新を有効にする

Secure Firewall Management CenterおよびSecure Firewall Device ManagerでCAバンドルの自動更新を有効にするには、次の手順を実行します。

1. SSHまたはコンソールを使用して、CLI経由でSFMCまたはSFDMにアクセスします。
2. 次のように、CLIでconfigure cert-update auto-update enableコマンドを実行します。

<#root>

```
> configure cert-update auto-update enable

Autoupdate is enabled and set for every day at 18:06 UTC
```

3. CAバンドルの更新が自動更新機能を備えているかどうかをテストするには、configure cert-update testコマンドを実行します。

```
<#root>

> configure cert-update test

Test succeeded, certs can safely be updated or are already up to date.
```

CAバンドルの更新を手動で実行

Secure Firewall Management CenterおよびSecure Firewall Device ManagerでCAバンドルの更新を手動で実行するには、次の手順を実行します。

1. SSHまたはコンソールを使用して、CLI経由でSFMCまたはSFDMにアクセスします。
2. 次のように、CLIでconfigure cert-update run-nowコマンドを実行します。

```
<#root>

> configure cert-update run-now

Certs have been replaced or was already up to date.
```

確認

CAバンドルの自動更新の検証

Secure Firewall Management CenterおよびSecure Firewall Device Manager上のCAバンドルの自動更新の設定を検証するには、次の手順を実行します。

1. SSHまたはコンソールを使用して、CLI経由でSFMCまたはSFDMにアクセスします。
2. CLIでshow cert-updateコマンドを実行します。

```
<#root>

> show cert-update


Autoupdate is enabled and set for every day at 18:06 UTC
CA bundle was last modified 'Wed Jul 19 03:11:31 2023'
```

トラブルシュート

更新エラー

推奨手順：

1. 現在のDNS設定を検証します。
2. 管理インターフェイスのインターネットとプロキシの設定を検証します。
3. ICMPを使用してtools.cisco.comとの接続を確認し、エキスパートモードでコマンドを使用してcurlを確認します。

```
sudo curl -vvk  https://tools.cisco.com
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。