配置FMC和FDM的CA捆綁的自動更新

目錄

簡介

本檔案介紹自動更新思科CA捆綁包用於Secure Firewall Management Center和Secure Firewall Device Manager的使用情況。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解思科安全防火牆管理中心（以前稱為Firepower管理中心）和安全防火牆裝置管理器（以前稱為Firepower裝置管理器）。
- 安全防火牆裝置（以前稱為Firepower）知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本7.0.5及更高版本的思科安全防火牆管理中心（FMC 1000、1600、2500、2600、4500、4600和虛擬）。
- 運行軟體版本7.1.0-3及更高版本的思科安全防火牆管理中心（FMC 1600、2600、4600和虛擬）。

- 思科安全防火牆管理中心（FMC 1600、2600、4600和虛擬），運行軟體版本7.2.4及更高版本。
- 運行軟體版本7.0.5及更高版本的思科安全防火牆（FPR 1000、2100、3100、4100、9300、ISA3000和虛擬），由安全防火牆裝置管理器管理。
- 運行軟體版本7.1.0-3及更高版本的思科安全防火牆（FPR 1000、2100、3100、4100、9300、ISA3000和虛擬），由安全防火牆裝置管理器管理。
- 運行軟體版本7.2.4及更高版本的思科安全防火牆（FPR 1000、2100、3100、4100、9300、ISA3000和虛擬），由安全防火牆裝置管理器管理。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科CA捆綁包的用途

思科安全防火牆（以前稱為Firepower）裝置使用包含證書的本地CA捆綁包來訪問多個思科服務（智慧許可、軟體、VDB、SRU和地理位置更新）。現在，系統會在系統定義的每日時間自動向思科查詢新的CA證書。之前，您必須升級軟體以更新CA證書。

附註：版本7.0.0至7.0.4、7.1.0至7.1.0-2或7.2.0至7.2.3不支援此功能。如果您從受支援的版本升級到不受支援的版本，則功能會暫時禁用，系統將會停止與思科聯絡。

為SFMC和SFDM上的CA捆綁包配置自動更新

啟用CA包的自動更新

要在Secure Firewall Management Center和Secure Firewall Device Manager上啟用CA捆綁的自動更新，請執行以下操作：

1. 使用SSH或控制檯訪問SFMC或SFDM over CLI。
2. 在CLI上運行configure cert-update auto-update enable命令：

<#root>

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

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

3.要測試CA捆綁包更新是否能夠自動更新，請運行configure cert-update test 命令：

<#root>

```
> configure cert-update test

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

手動運行CA捆綁包的更新

要在Secure Firewall Management Center和Secure Firewall Device Manager上手動運行CA捆綁包的更新，請執行以下操作：

1. 使用SSH或控制檯訪問SFMC或SFDM over CLI。
2. 在CLI上運行configure cert-update run-now 命令：

<#root>

```
> configure cert-update run-now

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

驗證

驗證CA捆綁包的自動更新

要驗證Secure Firewall Management Center和Secure Firewall Device Manager上CA捆綁包的自動更新配置，請執行以下操作：

1. 使用SSH或控制檯訪問SFMC或SFDM over CLI。
2. 在CLI上運行show cert-update 命令：

<#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'
```

疑難排解

更新錯誤

建議的步驟：

1. 驗證您當前的DNS配置。
2. 驗證管理介面的Internet和代理配置。

3. 使用ICMP確認您已與tools.cisco.com建立連線，並在專家模式下使用命令捲曲：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。