为FMC和FDM配置CA捆绑的自动更新

目录

简介

本文档介绍如何使用Cisco CA捆绑包自动更新安全防火墙管理中心和安全防火墙设备管理器。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解思科安全防火墙管理中心（以前称为Firepower管理中心）和安全防火墙设备管理器（以前称为Firepower设备管理器）。
- 安全防火墙设备（以前称为Firepower）知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本7.0.5及更高版本的思科安全防火墙管理中心（FMC 1000、1600、2500、2600、4500、4600和虚拟）。
- 运行软件版本7.1.0-3及更高版本的思科安全防火墙管理中心（FMC 1600、2600、4600和虚拟）。
- 运行软件版本7.2.4及更高版本的思科安全防火墙管理中心（FMC 1600、2600、4600和虚拟

）。
- 运行软件版本7.0.5及更高版本的思科安全防火墙（FPR 1000、2100、3100、4100、9300、ISA3000和虚拟），由安全防火墙设备管理器管理。
- 运行软件版本7.1.0-3及更高版本的思科安全防火墙（FPR 1000、2100、3100、4100、9300、ISA3000和虚拟），由安全防火墙设备管理器管理。
- 运行软件版本7.2.4及更高版本的思科安全防火墙（FPR 1000、2100、3100、4100、9300、ISA3000和虚拟），由安全防火墙设备管理器管理。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科CA捆绑包的用途

思科安全防火墙（以前称为Firepower）设备使用包含证书的本地CA捆绑包访问多个思科服务（智能许可、软件、VDB、SRU和地理位置更新）。现在，系统会在系统定义的每日时间自动向思科查询新的CA证书。以前，您必须升级软件以更新CA证书。

备注：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不支持此功能。如果您从支持的版本升级到不受支持的版本，则功能会暂时禁用，系统会停止与Cisco联系。

在SFMC和SFDM上配置CA捆绑的自动更新

为CA捆绑包启用自动更新

要启用Secure Firewall Management Center和Secure Firewall Device Manager上的CA捆绑的自动更新，请执行以下操作：

1. 使用SSH或控制台通过CLI访问SFMC或SFDM。
2. 在CLI上运行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.要测试CA捆绑包更新是否可以自动更新，请运行configure cert-update test命令：

<#root>

```
> configure cert-update test
```

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

手动运行CA捆绑包的更新

要在Secure Firewall Management Center和Secure Firewall Device Manager上手动运行CA捆绑包的更新，请执行以下操作：

1. 使用SSH或控制台通过CLI访问SFMC或SFDM。
2. 在CLI上运行configure cert-update run-now命令：

<#root>

```
> configure cert-update run-now

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

验证

验证CA捆绑包的自动更新

要验证安全防火墙管理中心和安全防火墙设备管理器上CA捆绑包自动更新的配置，请执行以下操作：

1. 使用SSH或控制台通过CLI访问SFMC或SFDM。
2. 在CLI上运行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'
```

故障排除

更新错误

建议步骤：

1. 验证您当前的DNS配置。
2. 验证管理接口的Internet和代理配置。
3. 在专家模式下使用ICMP确认您与tools.cisco.com连接，并使用curl命令确认连接：
   `sudo curl -vvk  https://tools.cisco.com`

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。