Automatische Aktualisierung von CA-Paketen für FMC und FDM konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die Verwendung der automatischen Aktualisierung der Cisco CA-Pakete für Secure Firewall Management Center und Secure Firewall Device Manager.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse des Cisco Secure Firewall Management Center (ehemals FirePOWER Management Center) und des Secure Firewall Device Manager (ehemals FirePOWER Device Manager)
- Secure Firewall Appliance (ehemals FirePOWER).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 und virtuell) mit Software-Version 7.0.5 und höher
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 und virtuell) mit der Software-Version 7.1.0-3 und höher
- Cisco Secure Firewall Management Center (FMC 1600, 2600,4600 und virtuell) mit der Software-Version 7.2.4 und höher
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 und virtuell) mit Softwareversion 7.0.5 und höher, verwaltet durch Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 und virtuell) mit Software-

Version 7.1.0-3 und höher, verwaltet durch Secure Firewall Device Manager

- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 und virtuell) mit Softwareversion 7.2.4 und höher, verwaltet durch Secure Firewall Device Manager.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Verwendung für Cisco CA-Pakete

Cisco Secure Firewall-Geräte (vormals FirePOWER) verwenden lokale CA-Pakete, die Zertifikate für den Zugriff auf mehrere Cisco Services (Smart Licensing, Software, VDB, SRU und Geolocation Updates) enthalten. Das System fragt Cisco nun automatisch nach neuen Zertifizierungsstellenzertifikaten zu einer vom System definierten Tageszeit ab. Bisher mussten Sie die Software aktualisieren, um Zertifizierungsstellenzertifikate zu aktualisieren.

Hinweis: Diese Funktion wird in den Versionen 7.0.0 bis 7.0.4, 7.1.0 bis 7.1.0-2 oder 7.2.0 bis 7.2.3 nicht unterstützt. Wenn Sie ein Upgrade von einer unterstützten auf eine nicht unterstützte Version durchführen, wird die Funktion vorübergehend deaktiviert, und das System stellt keine Verbindung zu Cisco mehr her.

Automatische Aktualisierung für CA-Pakete auf SFMC und SFDM konfigurieren

Automatisches Update für CA-Pakete aktivieren

So aktivieren Sie die automatische Aktualisierung für CA-Pakete im Secure Firewall Management Center und Secure Firewall Device Manager:

1. Zugriff auf SFMC oder SFDM über CLI mit SSH oder Konsole.
2. Führen Sie den Befehl **configure cert-update auto-update enable** in der CLI aus:

<#root>

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

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

3. Führen Sie den Befehl **configure cert-update test** aus, um zu testen, ob das CA Bundle Update automatisch aktualisiert werden kann:

<#root>

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

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

Aktualisierung für CA-Pakete manuell ausführen

So führen Sie die Aktualisierung für CA-Pakete auf Secure Firewall Management Center und Secure Firewall Device Manager manuell aus:

1. Zugriff auf SFMC oder SFDM über CLI mit SSH oder Konsole.
2. Führen Sie den Befehl **configure cert-update run-now** in der CLI aus:

<#root>

```
> configure cert-update run-now

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

Überprüfung

Validierung des automatischen Updates für CA-Pakete

So validieren Sie die Konfiguration für das automatische Update für CA-Pakete im Secure Firewall Management Center und Secure Firewall Device Manager:

1. Zugriff auf SFMC oder SFDM über CLI mit SSH oder Konsole.
2. Führen Sie den Befehl **show cert-update** in der CLI aus:

<#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'
```

Fehlerbehebung

Aktualisierungsfehler

Empfohlene Schritte

1. Validieren Sie Ihre aktuelle DNS-Konfiguration.
2. Validieren Sie die Internet- und Proxy-Konfiguration für die Management-Schnittstelle.
3. Stellen Sie sicher, dass Sie über ICMP eine Verbindung zu tools.cisco.com haben, und wechseln Sie mit dem Befehl im Expertenmodus:
   sudo curl -vvk https://tools.cisco.com

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.