Automatische update van CA-bundels voor FMC en FDM configureren

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Gebruik voor Cisco CA-bundels](#)
[Automatische update voor CA-bundels op SFMC en SFDM configureren](#)
[Automatische update voor CA-bundels inschakelen](#)
[De update voor CA-bundels handmatig uitvoeren](#)
[Verifiëren](#)
[De automatische update voor CA-bundels valideren](#)
[Problemen oplossen](#)
[Update fout](#)
[Aanbevolen stappen:](#)

Inleiding

Dit document beschrijft het gebruik van de automatische update van Cisco CA-bundels voor Secure Firewall Management Center en Secure Firewall Device Manager.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van Cisco Secure Firewall Management Center (voorheen bekend als Firepower Management Center) en Secure Firewall Device Manager (voorheen bekend als Firepower Device Manager).
- Kennis van Secure Firewall Applicatie (voorheen bekend als Firepower).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 en virtueel), actieve softwareversie 7.0.5 en hoger.
- Cisco Secure Firewall Management Center (FMC 1600, 2600,4600 en virtueel), actieve softwareversie 7.1.0-3 en hoger.
- Cisco Secure Firewall Management Center (FMC 1600, 2600,4600 en virtueel), actieve softwareversie 7.2.4 en hoger.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 en virtueel), actieve softwareversie 7.0.5 en hoger, beheerd door Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 en virtueel), actieve

softwareversie 7.1.0-3 en hoger, beheerd door Secure Firewall Device Manager.

- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 en virtueel), actieve softwareversie 7.2.4 en hoger, beheerd door Secure Firewall Device Manager.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Gebruik voor Cisco CA-bundels

Apparaten voor Cisco Secure Firewall (voorheen bekend als Firepower) maken gebruik van lokale CA-bundels die certificaten bevatten voor toegang tot verschillende Cisco-services (Smart Licensing, Software, VDB, SRU en Geolocation-updates). Het systeem vraagt nu automatisch Cisco om nieuwe CA-certificaten op een dagelijks door het systeem bepaald tijdstip. Eerder moest u de software upgraden om CA Certificaten bij te werken.

> **Opmerking**: Deze optie wordt niet ondersteund in versie 7.0.0 tot 7.0.4, 7.1.0 tot 7.1.0-2 of 7.2.0 tot 7.2.3. Als u een upgrade uitvoert van een ondersteunde versie naar een niet-ondersteunde versie, wordt de functie tijdelijk uitgeschakeld en stopt het systeem met contact opnemen met Cisco.

Automatische update voor CA-bundels op SFMC en SFDM configureren

Automatische update voor CA-bundels inschakelen

Automatische updates voor CA-bundels in Secure Firewall Management Center en Secure Firewall Device Manager inschakelen:

1. Toegang tot SFMC of SFDM via CLI met SSH of console.
2. Voer de opdracht **Enable** op CLI voor het configureren van **cert-update uit**:

<#root>

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

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

3. Om te testen of de CA-bundelupdate automatisch kan worden bijgewerkt, voert u de opdracht **Configure cert-update test uit**:

<#root>

```
> configure cert-update test

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

De update voor CA-bundels handmatig uitvoeren

U kunt als volgt de update voor CA-bundels handmatig uitvoeren op Secure Firewall Management Center en Secure Firewall Device Manager:

1. Toegang tot SFMC of SFDM via CLI met SSH of console.
2. Voer de opdracht **Configure cert-update run-now** op CLI uit:

<#root>

```
> configure cert-update run-now

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

Verifiëren

De automatische update voor CA-bundels valideren

U kunt als volgt de configuratie voor de automatische update van CA-bundels voor Secure Firewall Management Center en Secure Firewall Device Manager valideren:

1. Toegang tot SFMC of SFDM via CLI met SSH of console.
2. Start de **show cert-update** opdracht op CLI:

<#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'
```

Problemen oplossen

Update fout

Aanbevolen stappen:

1. Valideer uw huidige DNS-configuratie.
2. Bevestig de internet- en proxyconfiguratie voor de Management Interface.
3. Bevestig dat u connectiviteit met tools.cisco.com hebt die ICMP gebruiken en met het bevel in deskundige wijze krullen:
   sudo curl -vvk https://tools.cisco.com

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.