Configurer la mise à jour automatique des ensembles CA pour FMC et FDM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Utilisations pour les bundles Cisco CA

Configuration de la mise à jour automatique pour les ensembles CA sur SFMC et SFDM

- Activer la mise à jour automatique pour les bundles CA
- Exécuter manuellement la mise à jour des ensembles CA

Vérifier

- Valider la mise à jour automatique pour les ensembles CA

Dépannage

- Erreur de mise à jour
- Étapes recommandées :

Introduction

Ce document décrit l'utilisation de la mise à jour automatique des ensembles Cisco CA pour Secure Firewall Management Center et Secure Firewall Device Manager.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de Cisco Secure Firewall Management Center (anciennement Firepower Management Center) et de Secure Firewall Device Manager (anciennement Firepower Device Manager).
- Connaissances de l'appliance de pare-feu sécurisé (anciennement Firepower).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 et virtuel) exécutant la version logicielle 7.0.5 et ultérieure.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 et virtuel) exécutant le logiciel version 7.1.0-3 et ultérieure.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 et virtuel) exécutant le logiciel version 7.2.4 et ultérieure.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 et virtuel) exécutant la version logicielle 7.0.5 et ultérieure, gérée par Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 et virtuel) exécutant la version logicielle 7.1.0-3 et ultérieure, gérée par Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 et virtuel) exécutant la version logicielle 7.2.4 et ultérieure, gérée par Secure Firewall Device Manager.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Utilisations pour les bundles Cisco CA

Les périphériques Cisco Secure Firewall (anciennement Firepower) utilisent des bundles CA locaux contenant des certificats pour accéder à plusieurs services Cisco (licences Smart, logiciels, VDB, SRU et mises à jour de géolocalisation). Le système interroge désormais automatiquement Cisco pour obtenir de nouveaux certificats CA à une heure définie par le système. Auparavant, vous deviez mettre à niveau le logiciel pour mettre à jour les certificats CA.

Remarque: Cette fonctionnalité n'est pas prise en charge dans les versions 7.0.0 à 7.0.4, 7.1.0 à 7.1.0-2 ou 7.2.0 à 7.2.3. Si vous effectuez une mise à niveau d'une version prise en charge vers une version non prise en charge, la fonctionnalité est temporairement désactivée et le système cesse de contacter Cisco.

Configuration de la mise à jour automatique pour les ensembles CA sur SFMC et SFDM

Activer la mise à jour automatique pour les bundles CA

Pour activer la mise à jour automatique des ensembles CA sur Secure Firewall Management Center et Secure Firewall Device Manager :

1. Accédez à SFMC ou SFDM sur CLI en utilisant SSH ou Console.
2. Exécutez la commande configure cert-update auto-update enable dans l'interface de ligne de commande :

<#root>

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

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

3. Pour tester si la mise à jour de l'ensemble AC est capable de se mettre à jour automatiquement, exécutez la commande configure cert-update test :

<#root>

```
> configure cert-update test

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

Exécuter manuellement la mise à jour des ensembles CA

Pour exécuter manuellement les ensembles Mise à jour pour CA sur Secure Firewall Management Center et Secure Firewall Device Manager :

1. Accédez à SFMC ou SFDM sur CLI en utilisant SSH ou Console.
2. Exécutez la commande configure cert-update run-now sur CLI :

<#root>

```
> configure cert-update run-now

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

Vérifier

Valider la mise à jour automatique pour les ensembles CA

Pour valider la configuration des ensembles de mise à jour automatique pour CA sur Secure Firewall Management Center et Secure Firewall Device Manager :

1. Accédez à SFMC ou SFDM sur CLI en utilisant SSH ou Console.
2. Exécutez la commande show cert-update sur 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'
```

Dépannage

Erreur de mise à jour

Étapes recommandées :

1. Validez votre configuration DNS actuelle.
2. Validez la configuration Internet et proxy pour l'interface de gestion.
3. Vérifiez que vous disposez d'une connectivité avec tools.cisco.com à l'aide d'ICMP et utilisez la commande curl en mode expert :
   ```
   sudo curl -vvk  https://tools.cisco.com
   ```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.