Configuración de la actualización automática de los paquetes de CA para FMC y FDM

Contenido

Introducción

Este documento describe el uso de la actualización automática de Cisco CA Bundles para Secure Firewall Management Center y Secure Firewall Device Manager.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Cisco Secure Firewall Management Center (anteriormente conocido como Firepower Management Center) y Secure Firewall Device Manager (anteriormente conocido como Firepower Device Manager).
- Conocimiento de Secure Firewall Appliance (anteriormente conocido como Firepower).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 y virtual) que ejecuta la versión de software 7.0.5 y posterior.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 y virtual) que ejecuta la versión de software 7.1.0-3 y posterior.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 y virtual) que ejecuta la versión de software 7.2.4 y posterior.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 y virtual) que ejecuta la versión de software 7.0.5 y posterior, gestionada por Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 y virtual) que ejecuta la versión de software 7.1.0-3 y posterior, gestionada por Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 y virtual) que ejecuta la versión de software 7.2.4 y posterior, gestionada por Secure Firewall Device Manager.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Usos de los paquetes Cisco CA

Los dispositivos Cisco Secure Firewall (anteriormente conocidos como Firepower) utilizan paquetes de CA locales que contienen certificados para acceder a varios servicios de Cisco (licencias inteligentes, software, VDB, SRU y actualizaciones de geolocalización). El sistema ahora solicita automáticamente a Cisco nuevos certificados de CA a una hora diaria definida por el sistema. Anteriormente, tenía que actualizar el software para actualizar los certificados de CA.

Nota: esta función no se soporta en las versiones 7.0.0 a 7.0.4, 7.1.0 a 7.1.0-2, o 7.2.0 a 7.2.3. Si actualiza de una versión compatible a una versión no compatible, la función se deshabilita temporalmente y el sistema deja de ponerse en contacto con Cisco.

Configuración de la actualización automática para paquetes de CA en SFMC y SFDM

Habilitar actualización automática para paquetes de CA

Para habilitar la actualización automática para los paquetes de CA en Secure Firewall Management Center y Secure Firewall Device Manager:

1. Acceda a SFMC o SFDM a través de CLI mediante SSH o la consola.
2. Ejecute el comando configure cert-update auto-update enable en la CLI:

<#root>

> configure cert-update auto-update enable

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

3. Para probar si la actualización del paquete de CA es capaz de actualizarse automáticamente, ejecute el comando configure cert-update test:

<#root>

> configure cert-update test

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

Ejecutar la actualización para los paquetes de CA manualmente

Para ejecutar manualmente la actualización de los paquetes de CA en Secure Firewall Management Center y Secure Firewall Device Manager:

1. Acceda a SFMC o SFDM a través de CLI mediante SSH o la consola.
2. Ejecute el comando configure cert-update run-now en la CLI:

<#root>

> configure cert-update run-now

Certs have been replaced or was already up to date.

Verificación

Validar la actualización automática para los paquetes de CA

Para validar la configuración para la actualización automática para paquetes de CA en Secure Firewall Management Center y Secure Firewall Device Manager:

1. Acceda a SFMC o SFDM a través de CLI mediante SSH o la consola.
2. Ejecute el comando show cert-update en la 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'

Troubleshoot

Error de actualización

Pasos recomendados

1. Valide su configuración DNS actual.
2. Valide la configuración de Internet y proxy para la interfaz de administración.
3. Confirme que tiene conectividad con tools.cisco.com usando ICMP y rizar con el comando en el modo experto:
   ```
   sudo curl -vvk  https://tools.cisco.com
   ```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).