Configurar FMC para enviar registros de auditoría a un servidor Syslog

Contenido

Introducción

Este documento describe cómo configurar los registros de auditoría de Secure Firewall Management Center para enviarlos a un servidor Syslog.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Uso básico de Cisco Firewall Management Center (FMC)
- Comprensión del protocolo Syslog

Componentes Utilizados

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

- Cisco Firewall Management Center Virtual v7.4.0
- Servidor Syslog de terceros

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

Secure Firewall Management Center registra la actividad del usuario en registros de auditoría de solo lectura. A partir de Firepower versión 7.4.0, puede transmitir los cambios de configuración como parte de los datos del registro de auditoría a syslog especificando el formato de los datos de configuración y los hosts. La transmisión de los registros de auditoría a un servidor externo permite ahorrar espacio en el centro de gestión. Además, resulta útil cuando necesita proporcionar un seguimiento de auditoría de los cambios de configuración.

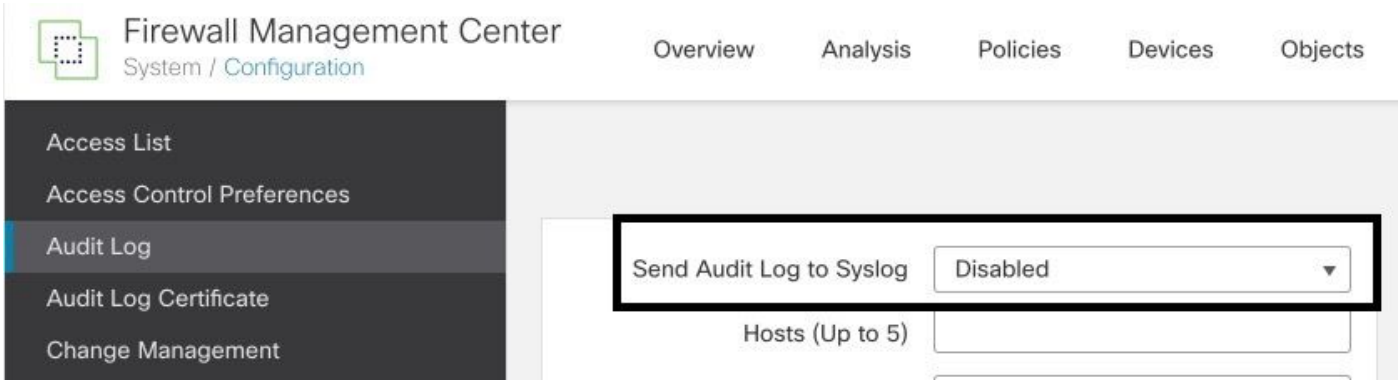
En caso de alta disponibilidad, solo el activo centro de administración envía los cambios de configuración de syslog a los servidores syslog externos. El archivo de registro se sincroniza entre los pares HA de modo que, durante una conmutación por error o conmutación, el nuevo centro de administración reanudaría el envío de los registros de cambios. En caso de que el par HA esté funcionando en modo de cerebro partido, ambos centro de administracións en el par envía el registro del sistema de cambio de configuración a los servidores externos.

Configurar

Paso 1. Registros de auditoría habilitados en Syslog

Para activar esta función de modo que FMC envíe los registros de auditoría a un servidor syslog, navegue hasta Sistema > Configuración > Registro de auditoría > Enviar registro de auditoría a Syslog > Activado.

Esta imagen muestra cómo habilitar la función Enviar registro de auditoría a Syslog:



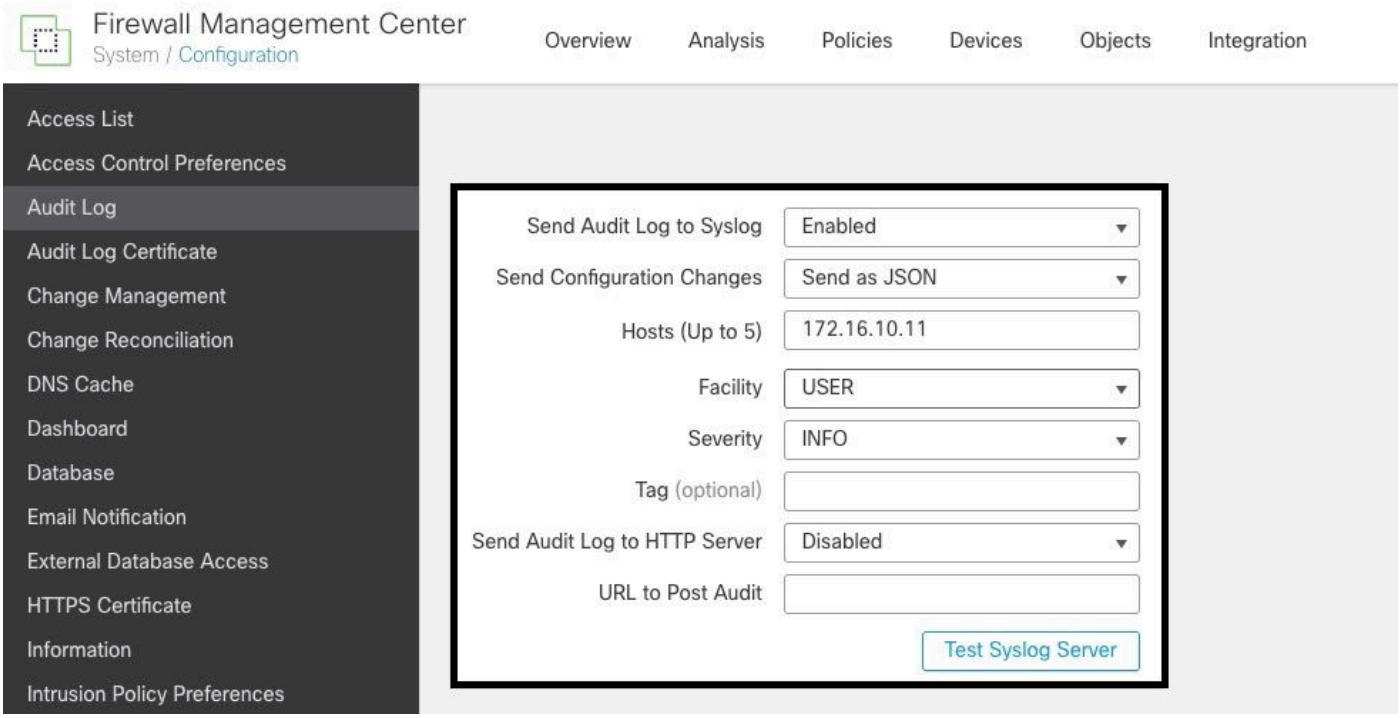
El FMC puede transmitir los datos del registro de auditoría a un máximo de cinco servidores syslog.

Paso 2. Configurar información de Syslog

Una vez habilitado el servicio, puede configurar la información de syslog. Para configurar la información de syslog, navegue hasta System > Configuration > Audit Log .

En función de sus requisitos, seleccione Enviar cambios de configuración, hosts, instalaciones y gravedad

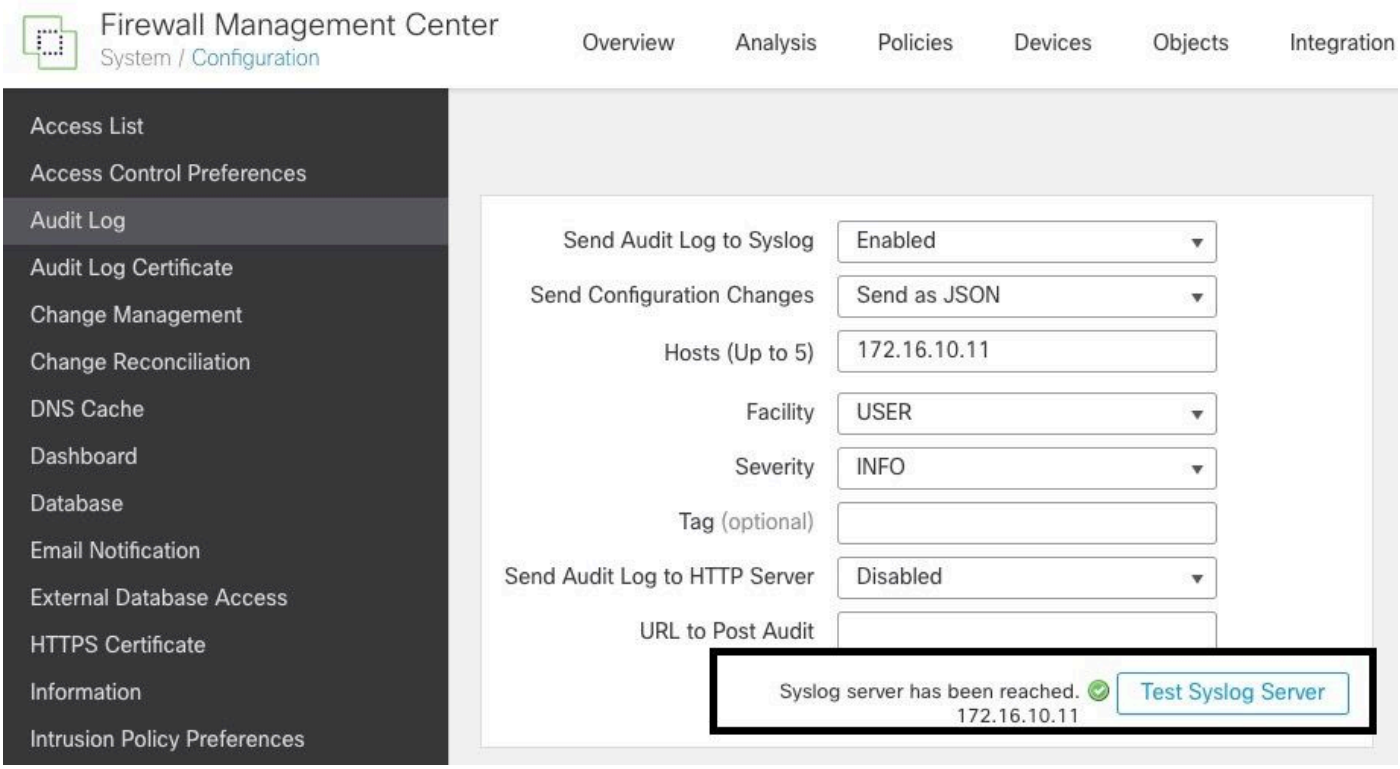
Esta imagen muestra los parámetros para configurar el servidor Syslog para los registros de auditoría:



Verificación

Para verificar si los parámetros están correctamente configurados, seleccione System > Configuration > Audit Log > Test Syslog Server .

Esta imagen muestra una prueba de servidor de Syslog exitosa:



Otra manera de verificar que syslog funciona, verifique la interfaz de syslog para confirmar que se están recibiendo los registros de auditoría.

Esta imagen muestra algunos ejemplos de los registros de auditoría recibidos por el servidor Syslog:

A continuación se muestran algunos ejemplos de los cambios de configuración que puede recibir en su servidor syslog:

```
2023-09-29 16:12:18 localhost 172.16.10.2 Sep 29 16:12:23 firepower: [FMC-AUDIT] mojo_server.pl: admin@
2023-09-29 16:12:20 localhost 172.16.10.2 Sep 29 16:12:25 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:12:23 localhost 172.16.10.2 Sep 29 16:12:28 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:13:39 localhost 172.16.10.2 Sep 29 16:13:44 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:32 localhost 172.16.10.2 Sep 29 16:14:37 firepower: [FMC-AUDIT] sfdccsm: admin@10.1.1.
2023-09-29 16:14:54 localhost 172.16.10.2 Sep 29 16:14:59 firepower: [FMC-AUDIT] ActionQueueScrape.pl:
2023-09-29 16:14:55 localhost 172.16.10.2 Sep 29 16:15:00 firepower: [FMC-AUDIT] ActionQueueScrape.pl:
```

Troubleshoot

Una vez aplicada la configuración, asegúrese de que FMC puede comunicarse con el servidor syslog.

El sistema utiliza paquetes ICMP/ARP y TCP SYN para verificar que el servidor syslog es accesible. Luego, el sistema usa de forma predeterminada el puerto 514/UDP para transmitir los registros de auditoría y el puerto TCP 1470 si protege el canal.

Para configurar una captura de paquetes en FMC, aplique estos comandos:

- tcpdump. Este comando captura el tráfico en la red

```
> expert
admin@firepower:~$ sudo su
Password:
```

```
root@firepower:/Volume/home/admin# tcpdump -i eth0 host 172.16.10.11 and port 514
```

Además, para probar la disponibilidad de ICMP, aplique este comando:

- ping. Este comando ayuda a confirmar si un dispositivo es accesible o no y a conocer la latencia de la conexión.

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin#ping 172.16.10.11
PING 172.16.10.11 (172.16.10.11) 56(84) bytes of data.
64 bytes from 172.16.10.11: icmp_seq=1 ttl=128 time=3.07 ms
64 bytes from 172.16.10.11: icmp_seq=2 ttl=128 time=2.06 ms
64 bytes from 172.16.10.11: icmp_seq=3 ttl=128 time=2.04 ms
64 bytes from 172.16.10.11: icmp_seq=4 ttl=128 time=0.632 ms
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- Guía de administración de Cisco Secure Firewall Management Center

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).