Configurar o FMC para enviar logs de auditoria a um Servidor Syslog

Contents

Introdução

Este documento descreve como configurar os Logs de Auditoria do Secure Firewall Management Center para serem enviados a um servidor Syslog.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Utilização básica do Cisco Firewall Management Center (FMC)
- Compreensão do protocolo Syslog

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Secure Firewall Management Center registra a atividade do usuário em logs de auditoria somente leitura. Iniciando o Firepower versão 7.4.0, você pode transmitir alterações de configuração como parte dos dados de log de auditoria para syslog especificando o formato dos dados de configuração e os hosts. A transmissão contínua de logs de auditoria para um servidor externo permite conservar espaço no centro de gerenciamento, bem como é útil quando você precisa fornecer uma trilha de auditoria das alterações de configuração.

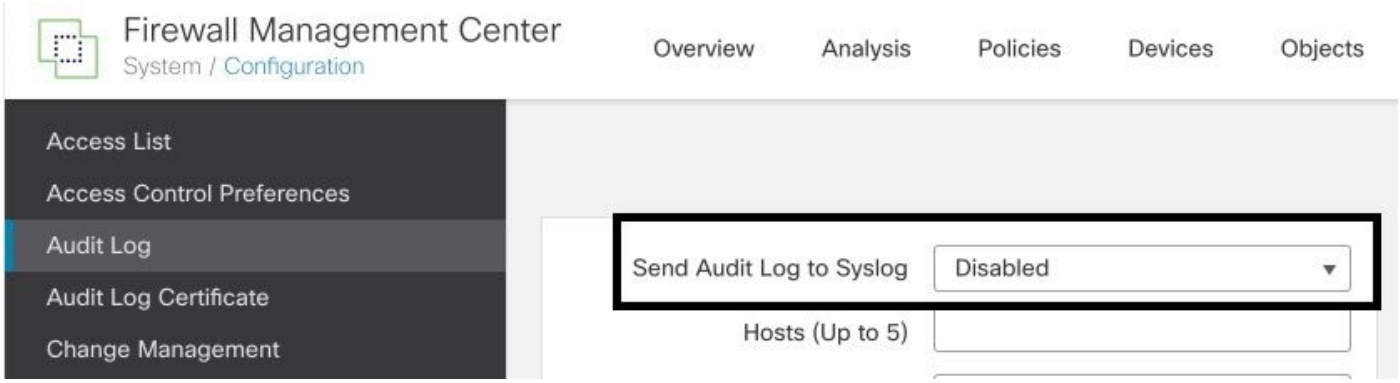
Em caso de alta disponibilidade, somente o ativo centro de gerenciamento envia o syslog de alterações de configuração para os servidores syslog externos. O arquivo de registro é sincronizado entre os pares de alta disponibilidade para que, durante um failover ou um switchover, o novo servidor centro de gerenciamento O retomaria o envio dos logs de alteração. Caso o par HA esteja funcionando em modo split brain, ambos centro de gerenciamentos no par envia o syslog de alteração de configuração para os servidores externos.

Configurar

Etapa 1. Logs de auditoria ativados para syslog

Para habilitar o FMC para que envie logs de auditoria para um Servidor syslog, navegue para System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled.

Esta imagem mostra como habilitar o recurso Enviar registro de auditoria para syslog:



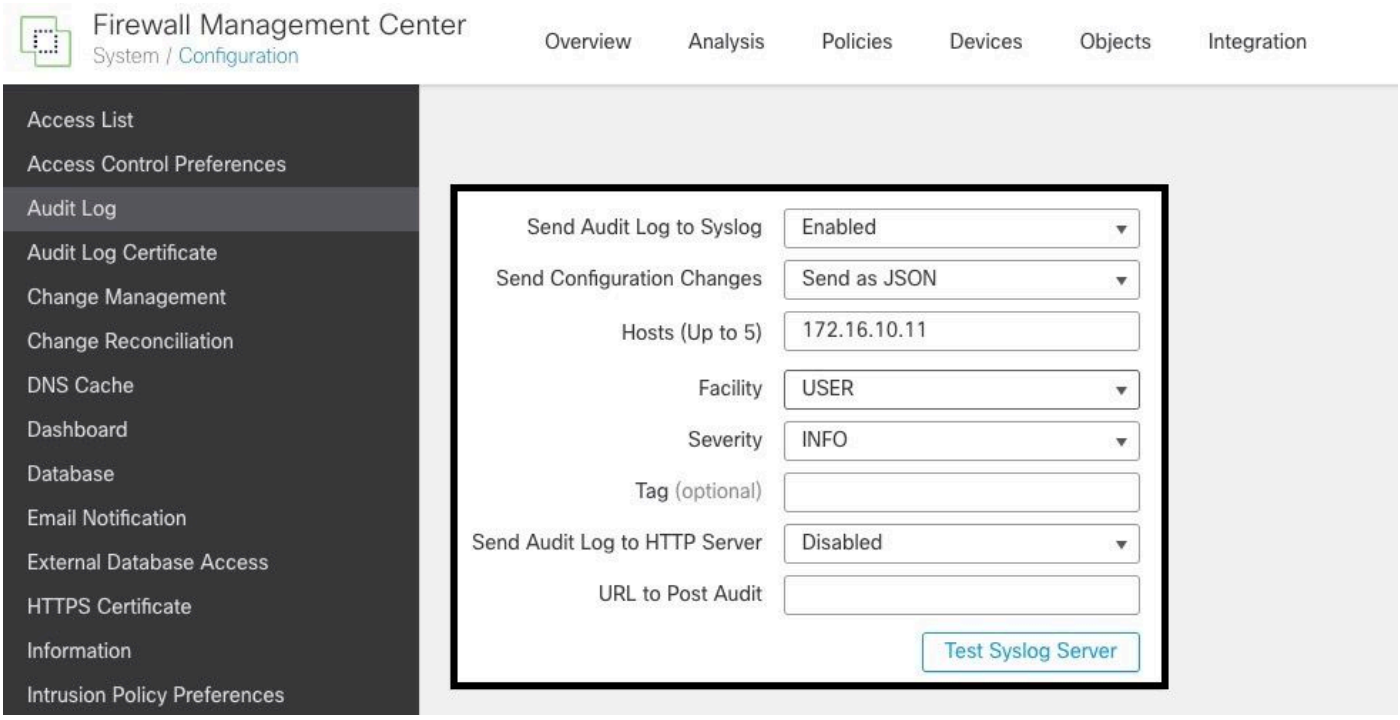
O FMC pode transmitir os dados do registro de auditoria para um máximo de cinco servidores syslog.

Etapa 2. Configurar informações de Syslog

Depois que o serviço for habilitado, você poderá configurar as informações de syslog. Para configurar as informações de syslog, navegue para System > Configuration > Audit Log.

Dependendo dos seus requisitos, selecione Send Configuration Changes, Hosts, Facility, Severity (Enviar alterações de configuração, hosts, instalações, gravidade)

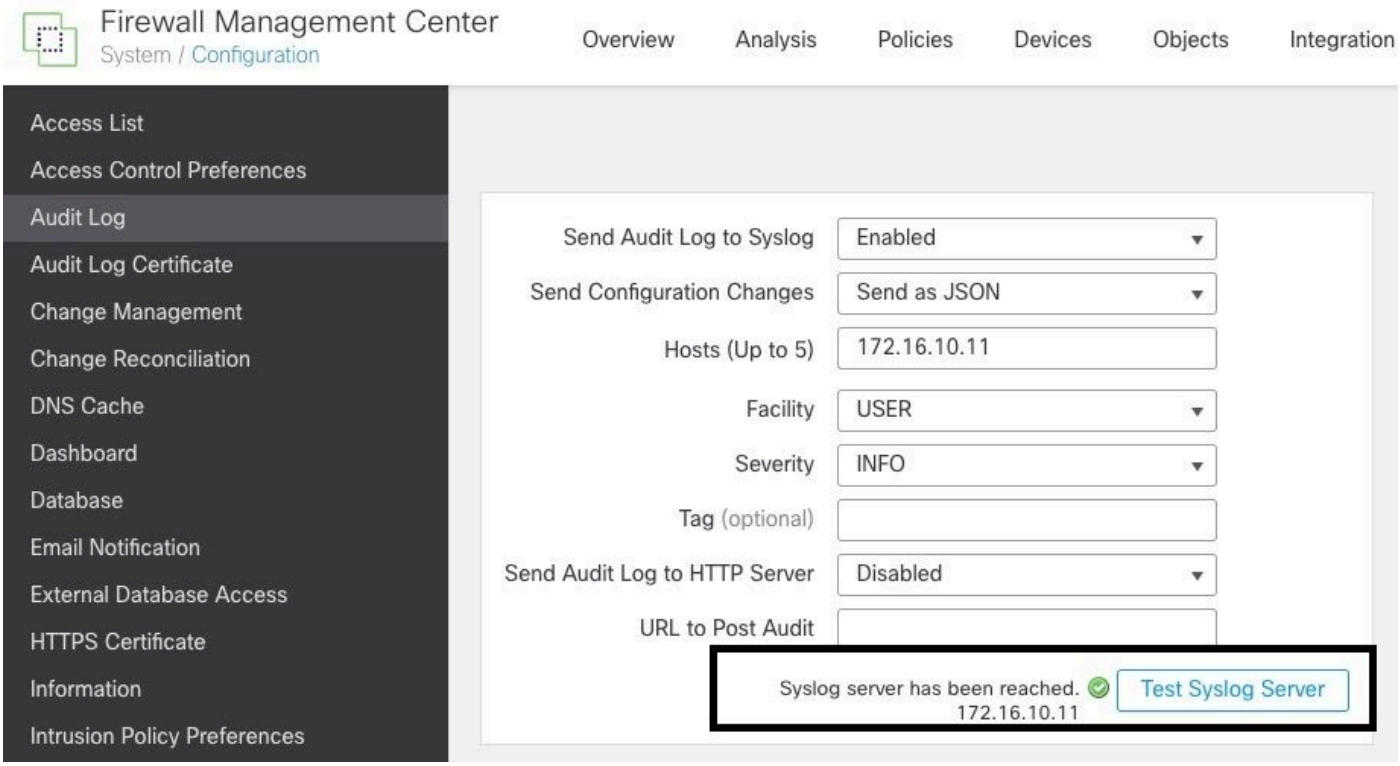
Esta imagem mostra os parâmetros para configurar o Servidor Syslog para Logs de Auditoria:



Verificar

Para verificar se os parâmetros estão configurados corretamente, selecione System > Configuration > Audit Log > Test Syslog Server.

Esta imagem mostra um Teste de Servidor Syslog bem-sucedido:



Outra maneira de verificar se o syslog está funcionando é verificar a interface do syslog para

confirmar se os logs de auditoria estão sendo recebidos.

Esta imagem mostra alguns exemplos dos logs de auditoria recebidos pelo Servidor Syslog:

Aqui estão alguns exemplos das alterações de configuração que você pode receber em seu 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:
```

Troubleshooting

Depois que a configuração tiver sido aplicada, verifique se o FMC pode se comunicar com o Servidor syslog.

O sistema usa os pacotes ICMP/ARP e TCP SYN para verificar se o Servidor syslog está acessível. Em seguida, por padrão, o sistema usa a porta 514/UDP para transmitir logs de auditoria e a porta TCP 1470 se você proteger o canal.

Para configurar uma captura de pacote no FMC, aplique estes comandos:

- TCP. Esse comando captura o tráfego na rede

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

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

Além disso, para testar a acessibilidade do ICMP, aplique este comando:

- ping. Esse comando ajuda a confirmar se um dispositivo está acessível ou não e a saber a latência da conexão.

```
> 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
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems
- Guia de administração do Cisco Secure Firewall Management Center

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.