

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

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Logs de auditoria ativados para syslog](#)

[Etapa 2. Configurar informações de Syslog](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## 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.

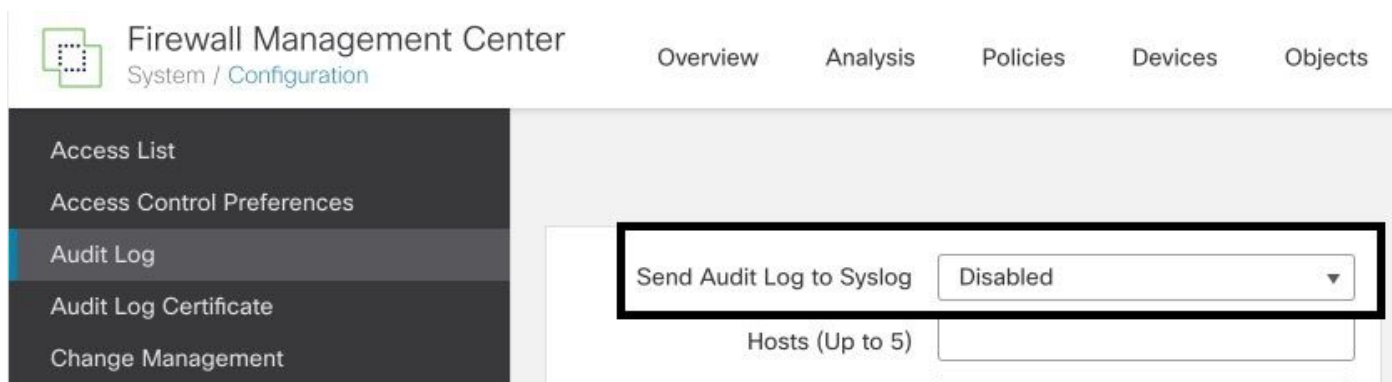
Em caso de alta disponibilidade, somente o ativo centro de gerenciamento envia o syslog de alterações de configuração para os servidores syslog externos. O arquivo de registro é sincronizado entre os pares de alta disponibilidade para que, durante um failover ou um switchover, o novo servidor centro de gerenciamento 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:

The screenshot shows the Firewall Management Center interface. The left sidebar contains a menu with items like Access List, Access Control Preferences, Audit Log (highlighted), Audit Log Certificate, Change Management, Change Reconciliation, DNS Cache, Dashboard, Database, Email Notification, External Database Access, HTTPS Certificate, Information, and Intrusion Policy Preferences. The main content area shows the configuration for Audit Log Syslog. A black box highlights the following settings: Send Audit Log to Syslog (Enabled), Send Configuration Changes (Send as JSON), Hosts (Up to 5) (172.16.10.11), Facility (USER), Severity (INFO), Tag (optional) (empty), Send Audit Log to HTTP Server (Disabled), and URL to Post Audit (empty). A Test Syslog Server button is visible at the bottom right of the configuration area.

## 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:

The screenshot shows the Firewall Management Center interface. The left sidebar is the same as in the previous image. The main content area shows the configuration for Audit Log Syslog. A black box highlights the Test Syslog Server button. Below the button, a message states: "Syslog server has been reached. ✓ 172.16.10.11".

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:

Date	Time	Priority	Hostname	Message
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1933"[19129] stunneldd stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: File copy 100 % completed, 40 bytes of file copied out of 40
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1932"[19129] stunneldd stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: cur_read=40, cur_write=40, total_bytes=40, stream_id_src=0, stream_id_dest=204, seq_id_src=1, seq_id_dest=1, state =Completed, started:2023 09 28 21:50:21 UTC, expires: 2023 09 28 22:00:21 UTC
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1931"[19129] stunneldd stream_file [INFO] FILE /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1930"[19129] stunneldd stream_file [INFO] ADDED INIT confirmation to be SRC: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1929"[19129] stunneldd stream_file [INFO] ADDED INIT confirmation to be SRC: cur_read=0, cur_write=0, total_bytes=0, stream_id_src=0, stream_id_dest=204, seq_id_src=0, seq_id_dest=0, state =Started, started:2023 09 28 21:50:21 UTC, expires: 2023 09 28 22:00:21 UTC
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1928"[19129] stunneldd stream_file [INFO] Adding SRC Task on Request, key: 0.204
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1927"[19129] stunneldd stream_file [INFO] Creating task on SRC for incoming task: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1926"[19129] stunneldd stream_file [INFO] Creating task on SRC for incoming task: cur_read=0, cur_write=0, total_bytes=0, stream_id_src=0, stream_id_dest=204, seq_id_src=0, seq_id_dest=0, state =Started, started:2023 09 28 21:50:21 UTC, expires: 2023 09 28 22:00:21 UTC
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1925"[19129] stunneldd stream_file [INFO] SRC TASK for KEY 0.204 was not found
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1924"[19129] stunneldd stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:16	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9755]: [meta sequenceld="1923"[19129] stunneldd stream_file [INFO] Sending message at /usr/local/sbin/pem/5.32.1/SFHealthMon pm line 579.
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1922"[19129] stunneldd stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: File copy 100 % completed, 42 bytes of file copied out of 42
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1921"[19129] stunneldd stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: cur_read=42, cur_write=42, total_bytes=42, stream_id_src=0, stream_id_dest=202, seq_id_src=1, seq_id_dest=1, state =Completed, started:2023 09 28 21:50:20 UTC, expires: 2023 09 28 22:00:20 UTC
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1920"[19129] stunneldd stream_file [INFO] FILE /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1919"[19129] stunneldd stream_file [INFO] ADDED INIT confirmation to be SRC: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1918"[19129] stunneldd stream_file [INFO] ADDED INIT confirmation to be SRC: cur_read=0, cur_write=0, total_bytes=0, stream_id_src=0, stream_id_dest=202, seq_id_src=0, seq_id_dest=0, state =Started, started:2023 09 28 21:50:20 UTC, expires: 2023 09 28 22:00:20 UTC
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1917"[19129] stunneldd stream_file [INFO] Adding SRC Task on Request, key: 0.202
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1916"[19129] stunneldd stream_file [INFO] Creating task on SRC for incoming task: File copy 0 % completed, 0 bytes of file copied out of 0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1915"[19129] stunneldd stream_file [INFO] Creating task on SRC for incoming task: cur_read=0, cur_write=0, total_bytes=0, stream_id_src=0, stream_id_dest=202, seq_id_src=0, seq_id_dest=0, state =Started, started:2023 09 28 21:50:20 UTC, expires: 2023 09 28 22:00:20 UTC
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1914"[19129] stunneldd stream_file [INFO] SRC TASK for KEY 0.202 was not found
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="1913"[19129] stunneldd stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9755]: [meta sequenceld="1912"[19129] stunneldd stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9755]: [meta sequenceld="1911"[19129] stunneldd stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:15	Local7/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9755]: [meta sequenceld="1910"[19129] stunneldd stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidsn_download/7cb124a4-4c0e-11ee-b245-a2990cda7a0
09-28-2023	21:50:07	Local7/Debug	172.16.10.2	Sep 28 21:50:12 firepower SF-IMS[9755]: [meta sequenceld="1909"[19129] stunneldd stream_file [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:50:05	Local7/Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9755]: [meta sequenceld="1908"[19129] stunneldd stream_file [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:50:05	Local7/Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9755]: [meta sequenceld="1907"[19129] stunneldd stream_file [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:49:57	User.Info	172.16.10.2	Sep 28 21:50:03 firepower: platformSettingFd.cgi: admin@10.152.201.95, System > Configuration > Configuration > /platform/platformSettingFd.cgi?type=AuditLog, Page View
09-28-2023	21:49:57	User.Info	172.16.10.2	Sep 28 21:50:02 firepower: ActionQueueScrape.pl: cron_processes@Default User IP, Login, Login Success
09-28-2023	21:49:57	Local7/Debug	172.16.10.2	Sep 28 21:50:02 firepower SF-IMS[9755]: [meta sequenceld="1907"[19129] stunneldd stream_file [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:49:57	Local7/Debug	172.16.10.2	Sep 28 21:50:02 firepower store_allowlist_history: [meta sequenceld="1906"[19129] stunneldd stream_file [INFO] store_allowlist_history finished successfully.
09-28-2023	21:49:56	Local7/Debug	172.16.10.2	Sep 28 21:50:01 firepower store_allowlist_history: [meta sequenceld="1905"[19129] stunneldd stream_file [INFO] invoking /usr/local/sbin/store_allowlist_history.pl.
09-28-2023	21:49:56	Local7/Debug	172.16.10.2	Sep 28 21:50:01 firepower CHROND[6894]: [meta sequenceld="1904"[19129] stunneldd stream_file [INFO] CMD [ /usr/libexec/sa/sa1 1 ]
09-28-2023	21:49:56	Local7/Debug	172.16.10.2	Sep 28 21:50:01 firepower CHROND[6893]: [meta sequenceld="1903"[19129] stunneldd stream_file [INFO] CMD [ /usr/local/sbin/run-parts-cron /etc/cron.5min ]
09-28-2023	21:49:56	User.Info	172.16.10.2	Sep 28 21:50:01 firepower: ActionQueueScrape.pl: admin@localhost, Task Queue, Policy Deployment to FTD - SUCCESS
09-28-2023	21:49:55	Local7/Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9755]: [meta sequenceld="1902"[19129] stunneldd stream_file [INFO] 16959378000.592.4011.310.867731.675066.010.000.005.100.00076.411152860.000.0000000.030.04002550.000.00060.030.030016107.411.410.0
09-28-2023	21:49:55	Local7/Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9755]: [meta sequenceld="1901"[19129] stunneldd stream_file [INFO] 16959378000.21221175000
09-28-2023	21:49:52	User.Info	172.16.10.2	Sep 28 21:49:57 firepower: audit_cen.cgi: admin@10.152.201.95, System > Configuration > Configuration > /admin/audit_cen.cgi, Page View

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:

## 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.