# FMC configureren voor verzenden van auditlogboeken naar een Syslog-server

## Inhoud



## Inleiding

Dit document beschrijft hoe u Secure Firewall Management Center-auditlogs kunt configureren om naar een Syslog-server te worden verzonden.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisbruikbaarheid van Cisco Firewall Management Center (FMC)
- Inzicht in het Syslog-protocol

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firewall Management Center virtuele versie 7.4.0
- Syslog-server van derden

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

Het Secure Firewall Management Center slaat gebruikersactiviteit op in alleen-lezen controlelogboeken. Als u Firepower versie 7.4.0 start, kunt u wijzigingen in de configuratie streamen als deel van de loggegevens van de audit naar syslog door het formaat van de configuratiegegevens en de hosts te specificeren. Het streamen van controlelogboeken aan een externe server staat u toe om ruimte op het beheerscentrum te besparen, eveneens, is het nuttig wanneer u controlespoor van configuratieveranderingen moet verstrekken.

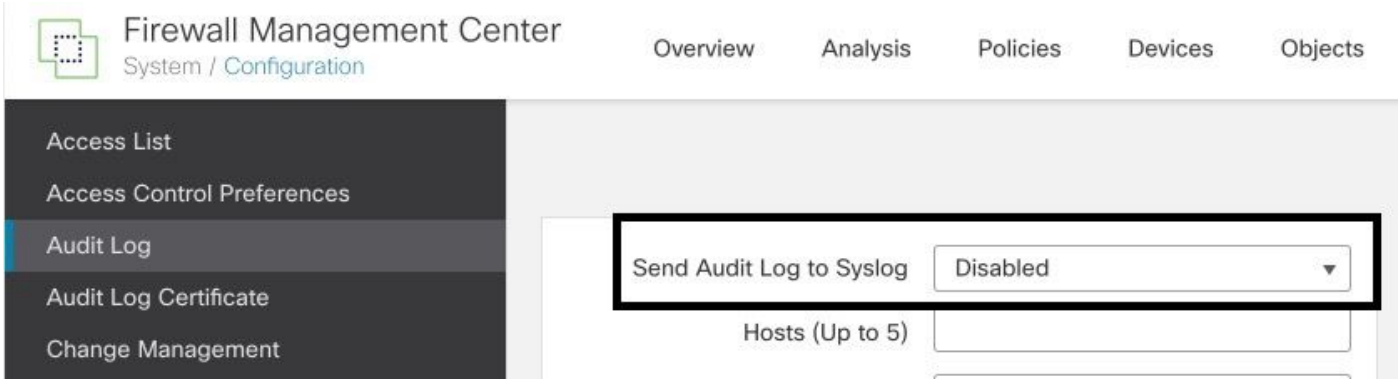
In geval van hoge beschikbaarheid, alleen de actieve beheerscentrum verzendt de configuratie wijzigingen syslog naar de externe syslog servers. Het logbestand is gesynchroniseerd tussen de HA-paren zodat tijdens een failover of switchover de nieuwe actieve beheerscentrum zou het verzenden van de veranderingslogboeken hervatten. Als het HA-paar werkt in de splitbreinmodus, zijn beide beheerscentrums in het paar verstuurt de configuratie verandering syslog naar de externe servers.

# Configureren

Stap 1. Toegelaten controlelogboeken aan Syslog

Om het VCC in te schakelen, stuurt u de controlelogboeken naar een syslog-server. Ga naar Systeem > Configuratie > Auditlogboek > Auditlogboek naar Syslog > Ingeschakeld.

Deze afbeelding toont hoe u de functie Auditlog naar Syslog verzenden kunt inschakelen:



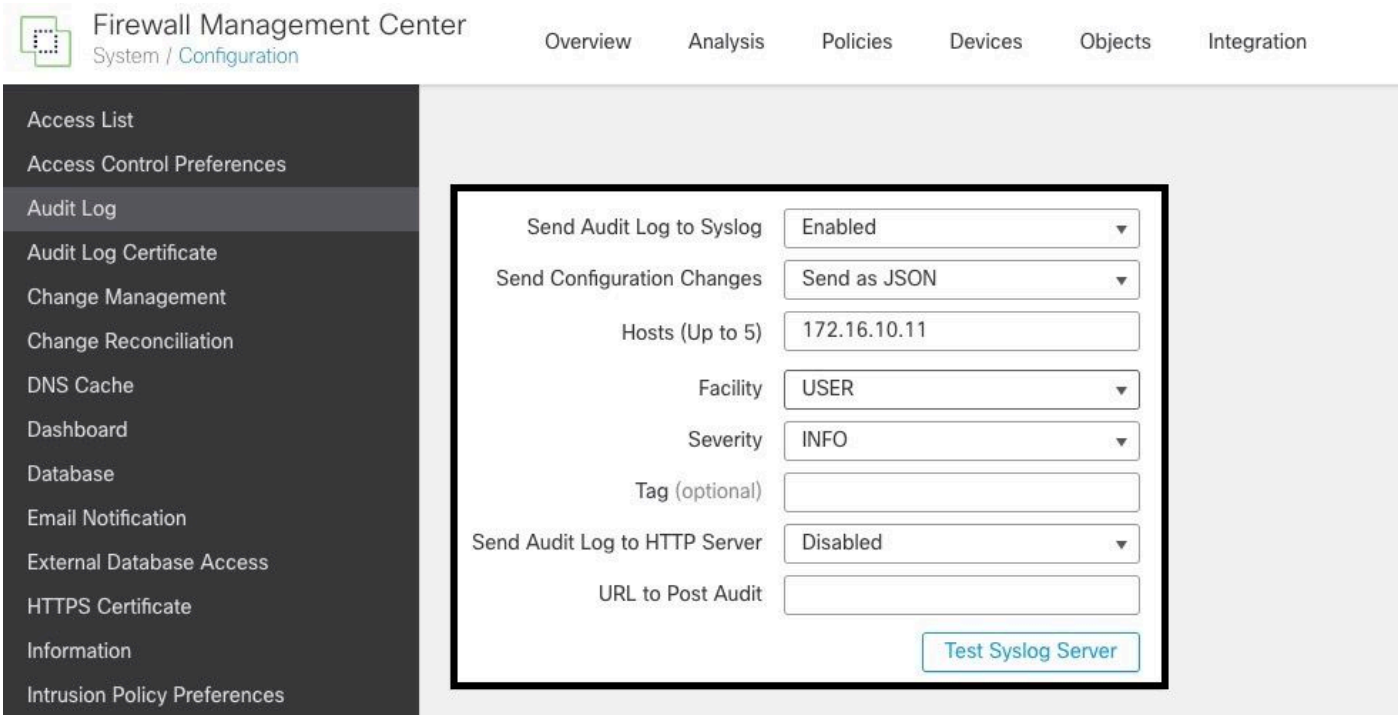

Het VCC kan de loggegevens van de audit streamen naar maximaal vijf syslog-servers.

Stap 2. Syslog-informatie configureren

Nadat de service is ingeschakeld, kunt u de syslog-informatie configureren. Om de sysloginformatie te configureren navigeert u naar Systeem > Configuratie > Auditlog.

Afhankelijk van uw vereisten selecteert u de optie Wijzigingen in configuratie verzenden, hosts, faciliteit, ernst

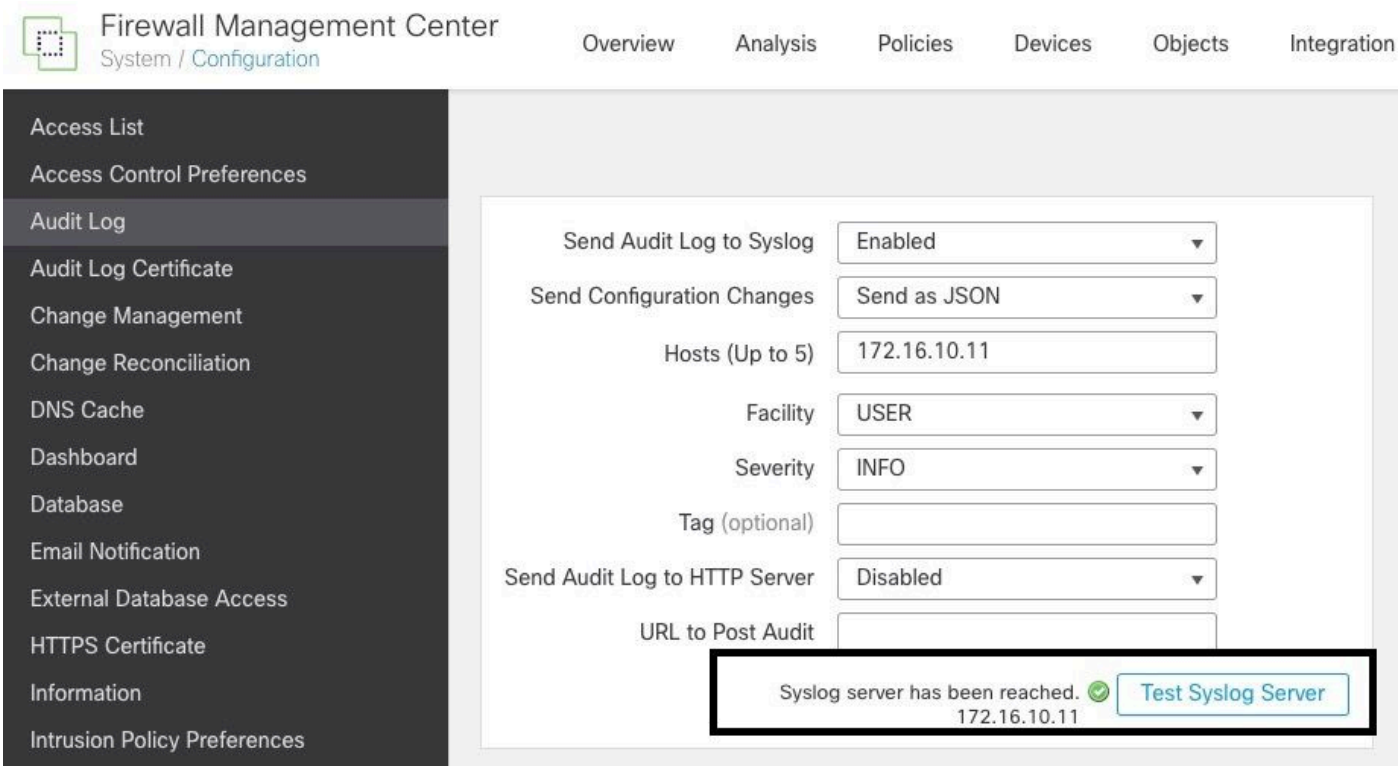
Dit beeld toont de parameters om Syslog Server voor Controlelogboeken te vormen:




# Verifiëren

Als u wilt controleren of de parameters correct zijn geconfigureerd, selecteert u Systeem > Configuratie > Auditlogboek > Syslog-server testen.

Deze afbeelding toont een succesvolle Syslog Server Test:




Een andere manier om te verifiëren dat syslog werkt, controleer de syslog interface om te bevestigen de controlelogboeken worden ontvangen.

Deze afbeelding toont enkele voorbeelden van de controlelogboeken die Syslog Server ontvangt:

| 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 sequenceId="1933"][19129] sfunneld: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 sequenceId="1932"][19129] sfunneld:stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: curr_read=40, curr_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 sequenceId="1931"][19129] sfunneld:stream_file [INFO] FILE /var/sf/sidns_download/7cb124a4-4c0e-11ee-b245-a2990cdac7a0 |
| 09-28-2023 | 21:50:16 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1930"][19129] sfunneld: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 sequenceId="1929"][19129] sfunneld:stream_file [INFO] ADDED INIT confirmation to be SRC: curr_read=0, curr_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 sequenceId="1928"][19129] sfunneld: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 sequenceId="1927"][19129] sfunneld: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 sequenceId="1926"][19129] sfunneld:stream_file [INFO] Creating task on SRC for incoming task: curr_read=0, curr_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 sequenceId="1925"][19129] sfunneld: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 sequenceId="1924"][19129] sfunneld:stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/sf/sidns_download/7cb124a4-4c0e-11ee-b245-a2990cdac7a0 |
| 09-28-2023 | 21:50:16 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:21 firepower SF-IMS[9765]: [meta sequenceId="1923"]run_hm[19200]: Sending message at /usr/local/sf/lib/perl/5.32.1/SF/HealthMon.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 sequenceId="1922"][19129] sfunneld: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 sequenceId="1921"][19129] sfunneld:stream_file [INFO] AFTER FOUND COMPL TASK ON SRC: curr_read=42, curr_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 sequenceId="1920"][19129] sfunneld:stream_file [INFO] FILE /var/sf/sidns_download/7cb2fa4a-4c0e-11ee-b245-a2990cdac7a0 |
| 09-28-2023 | 21:50:15 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1919"][19129] sfunneld: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 sequenceId="1918"][19129] sfunneld:stream_file [INFO] ADDED INIT confirmation to be SRC: curr_read=0, curr_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 sequenceId="1917"][19129] sfunneld: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 sequenceId="1916"][19129] sfunneld: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 sequenceId="1915"][19129] sfunneld:stream_file [INFO] Creating task on SRC for incoming task: curr_read=0, curr_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 sequenceId="1914"][19129] sfunneld: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 sequenceId="1913"][19129] sfunneld:stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/sf/sidns_download/7cb2fa4a-4c0e-11ee-b245-a2990cdac7a0 |
| 09-28-2023 | 21:50:15 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1912"]Seshat[10441]: 16959378200.8611.8214.3110.9407814.9214815.2210.0000.0004.7911.60[142.3980800.0000.0000800.0210.0600[2550.0000.0000600.0210.0400[6123.980.000.0 |
| 09-28-2023 | 21:50:15 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]EventIx[10442]: 1695937820[2122111750060 |
| 09-28-2023 | 21:50:07 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:12 firepower SF-IMS[9765]: [meta sequenceId="1910"]sshd_monitor[9974]: 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[9765]: [meta sequenceId="1909"]Seshat[10441]: 16959378101.0296.73032.5801.92110021.9086635.9000.0000.00011.71[1.60[367.2001527000.0000.0000000.0300.0500[2550.0000.0000600.0400.0400[6193.502.100.0 |
| 09-28-2023 | 21:50:05 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]EventIx[10442]: 1695937810[2122111750000 |
| 09-28-2023 | 21:49:58 | User.Info | 172.16.10.2 | Sep 28 21:50:03 firepower: platformSettingEdit.cgi: admin@10.152.201.95, System > Configuration > Configuration > /platinum/platformSettingEdit.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: csm_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[9765]: [meta sequenceId="1907"]sshd_monitor[9974]: 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 sequenceId="1906"]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 sequenceId="1905"]Invoking "/usr/local/sf/bin/store_allowlist_history.pl". |
| 09-28-2023 | 21:49:56 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:01 firepower CROND[6894]: [meta sequenceId="1904"](root) CMD (/usr/libexec/sa/sa1 1 1) |
| 09-28-2023 | 21:49:56 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:01 firepower CROND[6893]: [meta sequenceId="1903"](root) CMD ( /usr/local/sf/bin/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[9765]: [meta sequenceId="1902"]Seshat[10441]: 16959378000.5982.4611.3110.8607731.6705066.8110.0000.0005.1810.0076.41[1528680.0000.0000800.0300.0400[2550.0000.0000600.0300.0300[6107.401.400.0 |
| 09-28-2023 | 21:49:55 | Local7.Debug | 172.16.10.2 | Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]EventIx[10442]: 1695937800[2122111750000 |
| 09-28-2023 | 21:49:52 | User.Info | 172.16.10.2 | Sep 28 21:49:57 firepower: audit_cert.cgi: admin@10.152.201.95, System > Configuration > Configuration > /admin/audit_cert.cgi, Page View |

Hier zijn enkele voorbeelden van de configuratiewijzigingen die u in uw syslog-server kunt ontvangen:

```
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:
```

# Problemen oplossen

Zorg ervoor dat het VCC, nadat de configuratie is toegepast, kan communiceren met de syslogserver.

Het systeem gebruikt ICMP/ARP- en TCP/SYN-pakketten om te verifiëren dat de syslogserver bereikbaar is. Vervolgens gebruikt het systeem standaard poort 514/UDP om auditlogs en TCP-poort 1470 te streamen als u het kanaal beveiligd.

Pas de volgende opdrachten toe om een pakketopname op FMC te configureren:

- TCPdump. Deze opdracht legt het verkeer op het netwerk vast

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

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

Bovendien, om ICMP bereikbaarheid te testen, pas dit bevel toe:

- pingen. Deze opdracht helpt u te bevestigen of een apparaat al dan niet bereikbaar is en om de latentie van de verbinding te kennen.

```
> 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
```

# Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- Beheerdershandleiding voor Cisco Secure Firewall Management Center

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.