감사 로그를 Syslog 서버로 전송하도록 FMC 구성

목차

소개

이 문서에서는 Secure Firewall Management Center 감사 로그를 Syslog 서버로 전송하도록 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firewall Management Center)의 기본 사용 편의성
- Syslog 프로토콜 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firewall Management Center Virtual v7.4.0
- 서드파티 Syslog 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Secure Firewall Management Center는 사용자 활동을 읽기 전용 감사 로그에 기록합니다. Firepower 버전 7.4.0을 시작하면 컨피그레이션 데이터 형식 및 호스트를 지정하여 컨피그레이션 변경 사항을 감사 로그 데이터의 일부로 syslog에 스트리밍할 수 있습니다. 외부 서버로 감사 로그를 스트리밍하면 관리 센터의 공간을 절약할 수 있으며, 컨피그레이션 변경에 대한 감사 추적을 제공해야 하는 경우에도 유용합니다.

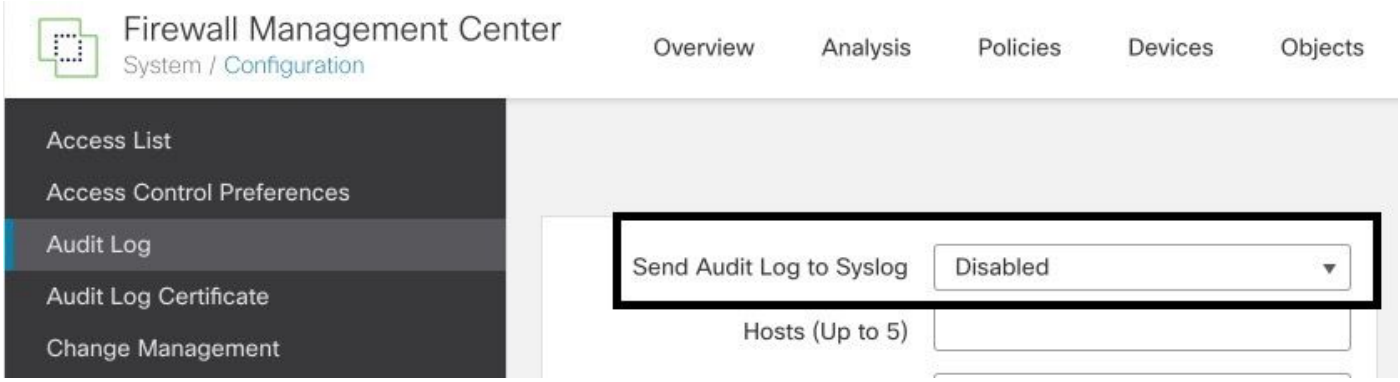
고가용성의 경우 관리 센터 외부 syslog 서버에 컨피그레이션 변경 syslog를 전송합니다. HA 쌍 간에 로그 파일이 동기화되어 장애 조치 또는 전환 중에 새 액티브 상태가 됩니다 관리 센터 변경 로그 전송을 다시 시작합니다. HA 쌍이 스플릿 브레인 모드에서 작동하는 경우 둘 다 관리 센터쌍의 는 외부 서버에 컨피그레이션 변경 syslog를 전송합니다.

구성

1단계. Syslog에 대한 감사 로그 사용

FMC에서 감사 로그를 syslog 서버로 전송하도록 활성화하려면 System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled로 이동합니다.

이 그림에서는 Send Audit Log to Syslog(Syslog에 감사 로그 보내기) 기능을 활성화하는 방법을 보여 줍니다.



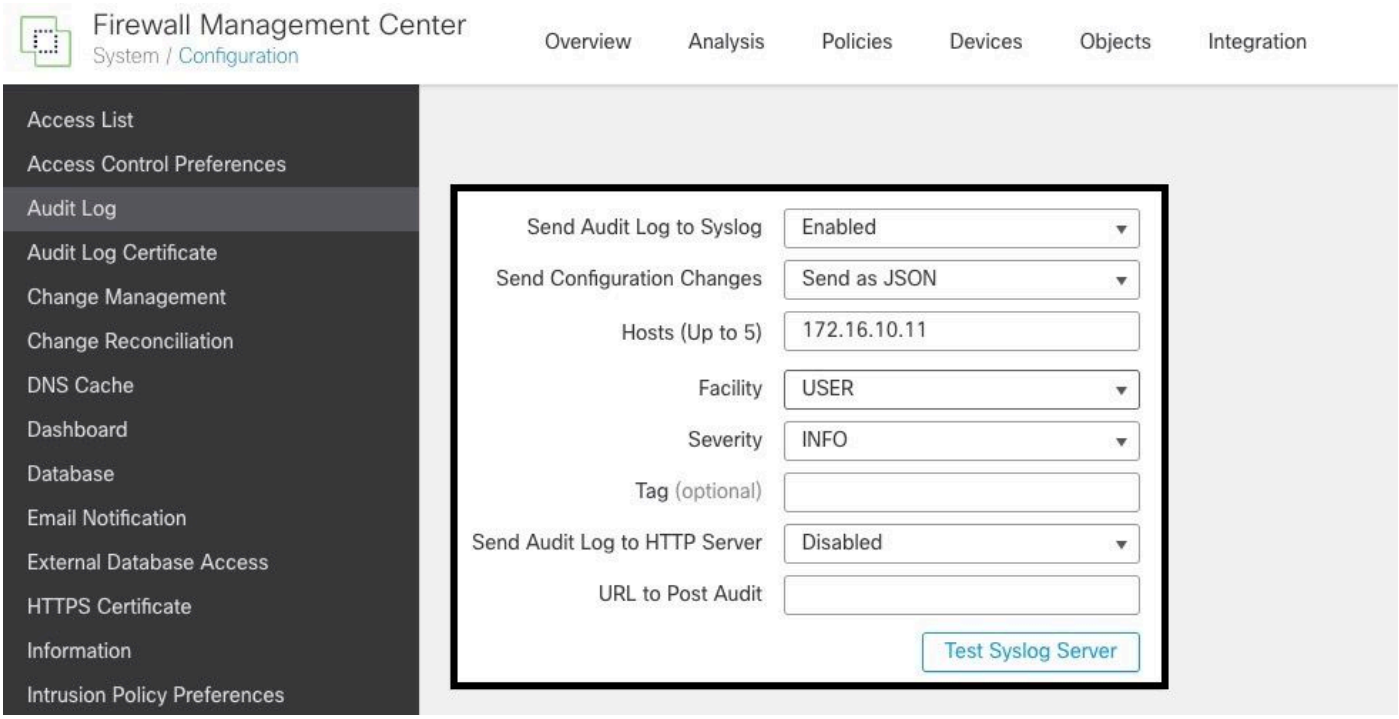
FMC는 감사 로그 데이터를 최대 5개의 syslog 서버로 스트리밍할 수 있습니다.

2단계. Syslog 정보 구성

서비스를 활성화한 후에는 syslog 정보를 구성할 수 있습니다. syslog 정보를 구성하려면 System > Configuration > Audit Log로 이동합니다.

요구 사항에 따라 Send Configuration Changes, Hosts, Facility, Severity를 선택합니다

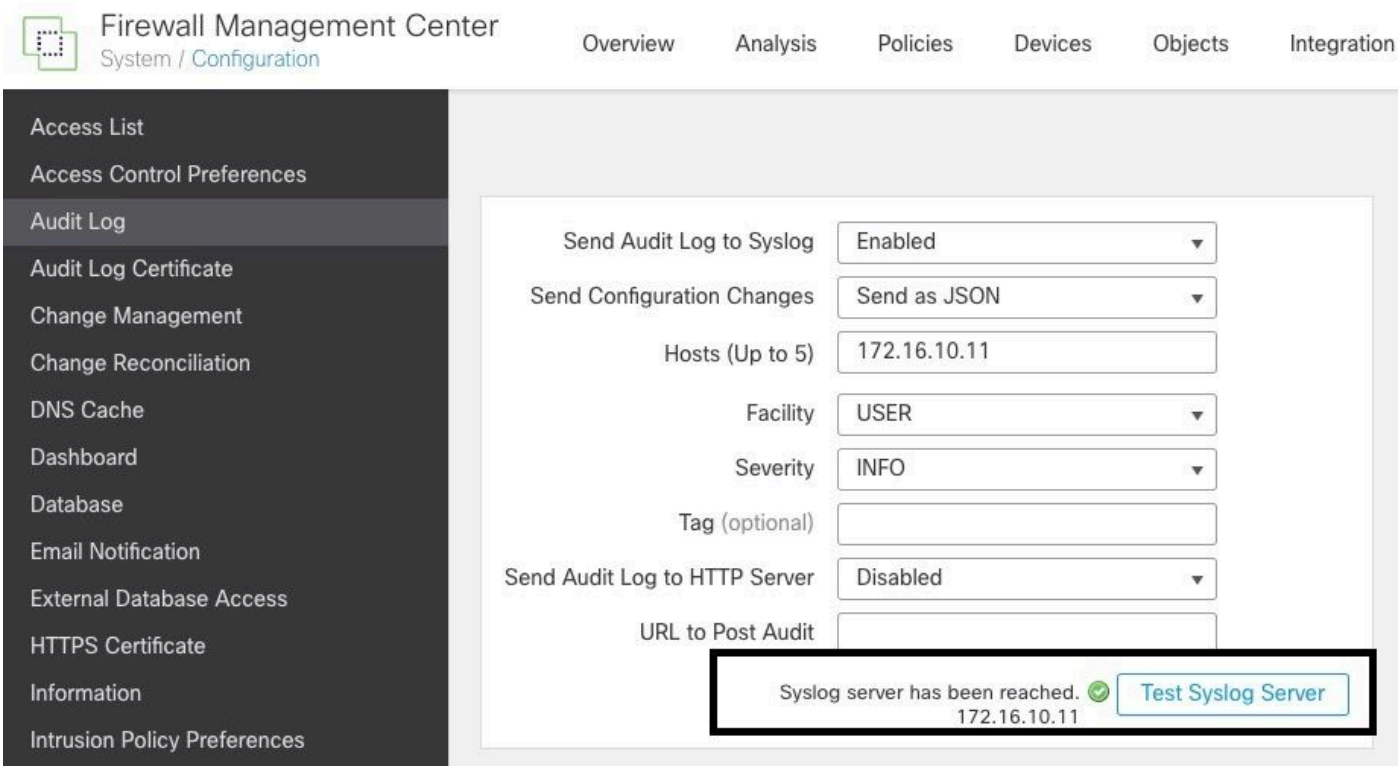
이 그림에서는 감사 로그에 대해 Syslog 서버를 구성하는 매개변수를 보여줍니다.



다음을 확인합니다.

매개변수가 올바르게 구성되었는지 확인하려면 System > Configuration > Audit Log > Test Syslog Server를 선택합니다.

이 그림에서는 성공적인 Syslog 서버 테스트를 보여 줍니다.



syslog가 작동 중인지 확인하는 또 다른 방법은 syslog 인터페이스를 확인하여 감사 로그를 수신하는지 확인합니다.

이 그림에서는 Syslog 서버에서 받은 감사 로그의 몇 가지 예를 보여 줍니다.


<table>
<tr><th>Date</th><th>Time</th><th>Priority</th><th>Hostname</th><th>Message</th></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1933"][19129] sftunneld:stream_file [INFO] AFTER FOUND COMPL TASK ON SRC:: File copy 100 % completed, 40 bytes of file copied out of 40</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1932"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1931"][19129] sftunneld:stream_file [INFO] FILE /var/sf/sidns_download/7cb124a4-4c0e-11ee-b245-a2990cdac7a0</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1930"][19129] sftunneld:stream_file [INFO] ADDED INIT confirmation to be SRC:: File copy 0 % completed, 0 bytes of file copied out of 0</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1929"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1928"][19129] sftunneld:stream_file [INFO] Adding SRC Task on Request, key: 0:204</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1927"][19129] sftunneld:stream_file [INFO] Creating task on SRC for incoming task:: File copy 0 % completed, 0 bytes of file copied out of 0</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1926"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1925"][19129] sftunneld:stream_file [INFO] SRC TASK for KEY 0:204 was not found</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="1924"][19129] sftunneld:stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/sf/sidns_download/7cb124a4-4c0e-11ee-b245-a2990cdac7a0</td></tr>
<tr><td>09-28-2023</td><td>21:50:16</td><td>Local7.Debug</td><td>172.16.10.2</td><td>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.</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1922"][19129] sftunneld:stream_file [INFO] AFTER FOUND COMPL TASK ON SRC:: File copy 100 % completed, 42 bytes of file copied out of 42</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1921"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1920"][19129] sftunneld:stream_file [INFO] FILE /var/sf/sidns_download/7cb2fa4a-4c0e-11ee-b245-a2990cdac7a0</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1919"][19129] sftunneld:stream_file [INFO] ADDED INIT confirmation to be SRC:: File copy 0 % completed, 0 bytes of file copied out of 0</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1918"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1917"][19129] sftunneld:stream_file [INFO] Adding SRC Task on Request, key: 0:202</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1916"][19129] sftunneld:stream_file [INFO] Creating task on SRC for incoming task:: File copy 0 % completed, 0 bytes of file copied out of 0</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1915"][19129] sftunneld: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</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1914"][19129] sftunneld:stream_file [INFO] SRC TASK for KEY 0:202 was not found</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceId="1913"][19129] sftunneld:stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/sf/sidns_download/7cb2fa4a-4c0e-11ee-b245-a2990cdac7a0</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1912"]Seshat[10441]: 1695937820|0.86|1.82|4.31|0.94|7814.92|4815.22|0.00|0.00|4.79|1.60|142.39|0|0|0.00|0.00|0|0|0.02|0.06|0|255|0.00|0.00|0|6|0.02|0.04|0|16|23.9|0.0|0.0</td></tr>
<tr><td>09-28-2023</td><td>21:50:15</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]Eventds[10442]: 1695937820|2|122|1175|0|60</td></tr>
<tr><td>09-28-2023</td><td>21:50:07</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:12 firepower SF-IMS[9765]: [meta sequenceId="1910"]sshd_monitor[9974]: sshd is running with 2046 4005 3992 2046</td></tr>
<tr><td>09-28-2023</td><td>21:50:05</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1909"]Seshat[10441]: 1695937810|1.02|6.73|32.58|1.92|10021.90|6635.90|0.00|0.00|11.71|1.60|367.20|15|278|0.00|0.00|0|0|0.03|0.05|0|255|0.00|0.00|0|6|0.04|0.04|0|16|193.5|2.1|0.0</td></tr>
<tr><td>09-28-2023</td><td>21:50:05</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]Eventds[10442]: 1695937810|2|122|1175|0|0</td></tr>
<tr><td>09-28-2023</td><td>21:49:58</td><td>User.Info</td><td>172.16.10.2</td><td>Sep 28 21:50:03 firepower: platformSettingEdit.cgi: admin@10.152.201.95, System > Configuration > Configuration > /platinum/platformSettingEdit.cgi?type=AuditLog, Page View</td></tr>
<tr><td>09-28-2023</td><td>21:49:57</td><td>User.Info</td><td>172.16.10.2</td><td>Sep 28 21:50:02 firepower: ActionQueueScrape.pl: csm_processes@Default User IP, Login, Login Success</td></tr>
<tr><td>09-28-2023</td><td>21:49:57</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:02 firepower SF-IMS[9765]: [meta sequenceId="1907"]sshd_monitor[9974]: sshd is running with 2046 4005 3992 2046</td></tr>
<tr><td>09-28-2023</td><td>21:49:57</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:02 firepower store_allowlist_history: [meta sequenceId="1906"]store_allowlist_history finished successfully.</td></tr>
<tr><td>09-28-2023</td><td>21:49:56</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:01 firepower store_allowlist_history: [meta sequenceId="1905"]Invoking '/usr/local/sf/bin/store_allowlist_history.pl'.</td></tr>
<tr><td>09-28-2023</td><td>21:49:56</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:01 firepower CROND[6894]: [meta sequenceId="1904"](root) CMD (/usr/libexec/sa/sa1 1 1)</td></tr>
<tr><td>09-28-2023</td><td>21:49:56</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:01 firepower CROND[6893]: [meta sequenceId="1903"](root) CMD (/usr/local/sf/bin/run-parts-cron /etc/cron.5min)</td></tr>
<tr><td>09-28-2023</td><td>21:49:56</td><td>User.Info</td><td>172.16.10.2</td><td>Sep 28 21:50:01 firepower: ActionQueueScrape.pl: admin@localhost, Task Queue, Policy Deployment to FTD - SUCCESS</td></tr>
<tr><td>09-28-2023</td><td>21:49:55</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1902"]Seshat[10441]: 1695937800|0.59|2.46|11.31|0.86|7731.67|5066.81|0.00|0.00|5.18|0.00|76.41|15|286|0.00|0.00|0|0|0.03|0.04|0|255|0.00|0.00|0|6|0.03|0.03|0|16|107.4|1.4|0.0</td></tr>
<tr><td>09-28-2023</td><td>21:49:55</td><td>Local7.Debug</td><td>172.16.10.2</td><td>Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]Eventds[10442]: 1695937800|2|122|1175|0|0</td></tr>
<tr><td>09-28-2023</td><td>21:49:52</td><td>User.Info</td><td>172.16.10.2</td><td>Sep 28 21:49:57 firepower: audit_cert.cgi: admin@10.152.201.95, System > Configuration > Configuration > /admin/audit_cert.cgi, Page View</td></tr>
</table>

다음은 syslog 서버에서 수신할 수 있는 컨피그레이션 변경의 몇 가지 예입니다.

```
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:
```

문제 해결

컨피그레이션이 적용된 후 FMC가 syslog 서버와 통신할 수 있는지 확인합니다.

시스템은 ICMP/ARP 및 TCP SYN 패킷을 사용하여 syslog 서버에 연결할 수 있는지 확인합니다. 그러면 기본적으로 시스템은 포트 514/UDP를 사용하여 감사 로그를 스트리밍하고, 채널을 보호하는 경우 TCP 포트 1470을 사용합니다.

FMC에서 패킷 캡처를 구성하려면 다음 명령을 적용합니다.

- tcpdump. 이 명령은 네트워크의 트래픽을 캡처합니다

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

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

또한 ICMP 연결성을 테스트하려면 다음 명령을 적용합니다.

- ping을 실행합니다. 이 명령은 디바이스가 연결 가능한지 확인하고 연결의 레이턴시를 파악하는 데 도움이 됩니다.

```
> 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
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- Cisco Secure Firewall Management Center 관리 설명서

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.