Konfigurieren von FMC zum Senden von Audit-Protokollen an einen Syslog-Server

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Überwachungsprotokolle von Secure Firewall Management Center konfiguriert werden, die an einen Syslog-Server gesendet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende Benutzerfreundlichkeit des Cisco Firewall Management Center (FMC)
- Verständnis des Syslog-Protokolls

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firewall Management Center Virtual v7.4.0
- Syslog-Server von Drittanbietern

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Secure Firewall Management Center zeichnet Benutzeraktivitäten in schreibgeschützten Audit-Protokollen auf. Ab Firepower 7.4.0 können Sie Konfigurationsänderungen als Teil der Prüfprotokolldaten in Syslog streamen, indem Sie das Konfigurationsdatenformat und die Hosts angeben. Durch das Streaming von Prüfprotokollen an einen externen Server können Sie außerdem Platz im Management Center sparen. Dies ist nützlich, wenn Sie Prüfprotokolle von Konfigurationsänderungen bereitstellen müssen.

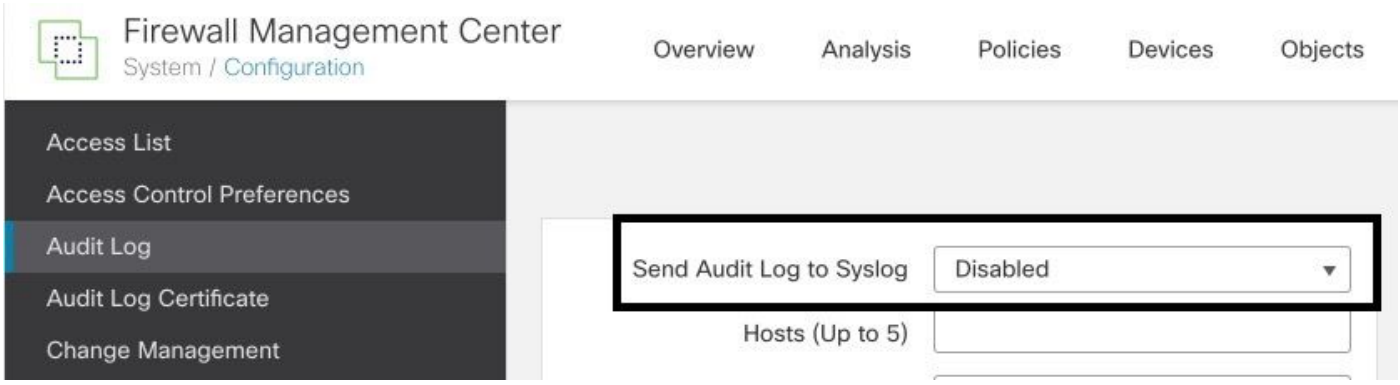
Bei hoher Verfügbarkeit wird nur der aktive Verwaltungszentrum sendet die Konfigurationsänderungs-Syslog an die externen Syslog-Server. Die Protokolldatei wird zwischen den HA-Paaren synchronisiert, sodass bei einem Failover oder Switchover die neue aktive Verwaltungszentrum würde das Senden der Änderungsprotokolle fortsetzen. Falls das HA-Paar im Split-Brain-Modus arbeitet, Verwaltungszentrums des Paars sendet das Konfigurationsänderungs-Syslog an die externen Server.

Konfigurieren

Schritt 1: Überwachungsprotokolle für Syslog aktiviert

Um diese Funktion zu aktivieren, damit FMC Prüfprotokolle an einen Syslog-Server sendet, navigieren Sie zu System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled.

Dieses Bild zeigt, wie Sie die Funktion "Prüfprotokoll an Syslog senden" aktivieren:



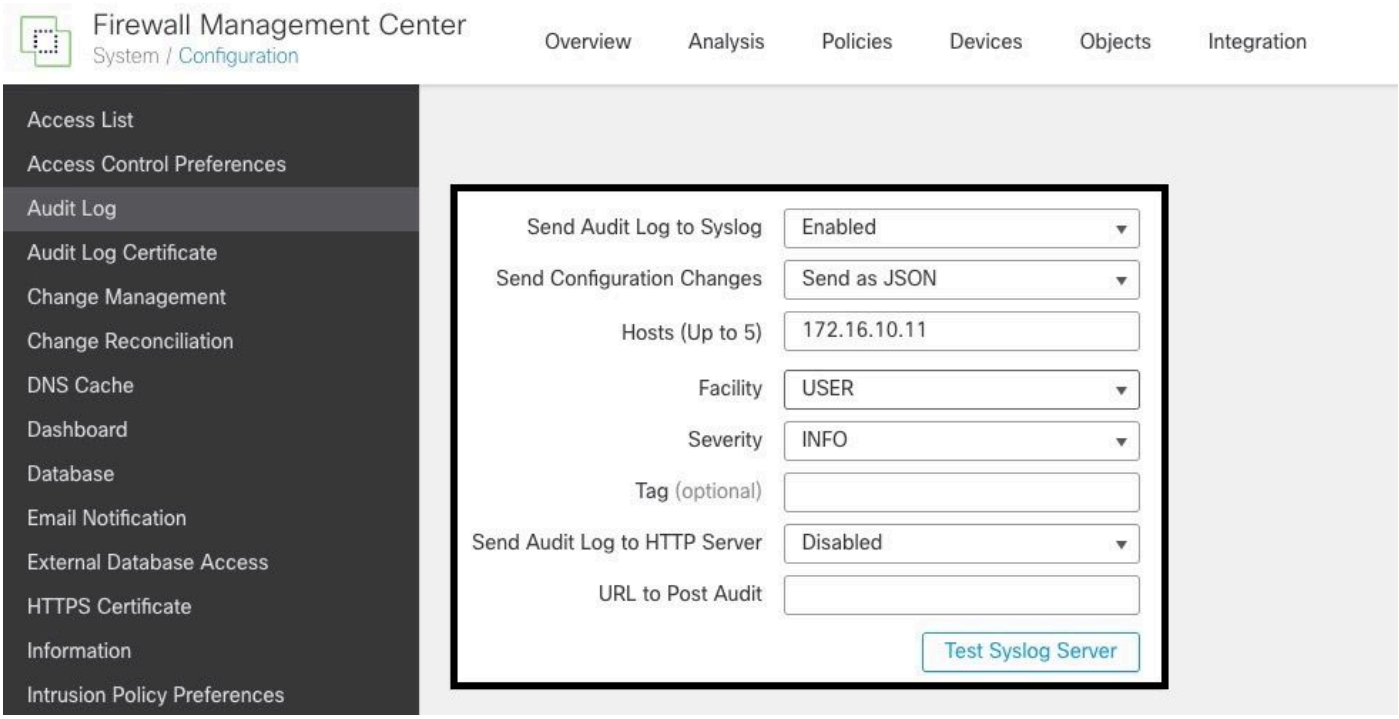
Das FMC kann Prüfprotokolldaten an maximal fünf Syslog-Server streamen.

Schritt 2: Syslog-Informationen konfigurieren

Nachdem der Service aktiviert wurde, können Sie die Syslog-Informationen konfigurieren. Um die Syslog-Informationen zu konfigurieren, navigieren Sie zu System > Configuration > Audit Log.

Wählen Sie je nach Anforderungen Send Configuration Changes, Hosts, Facility, Severity

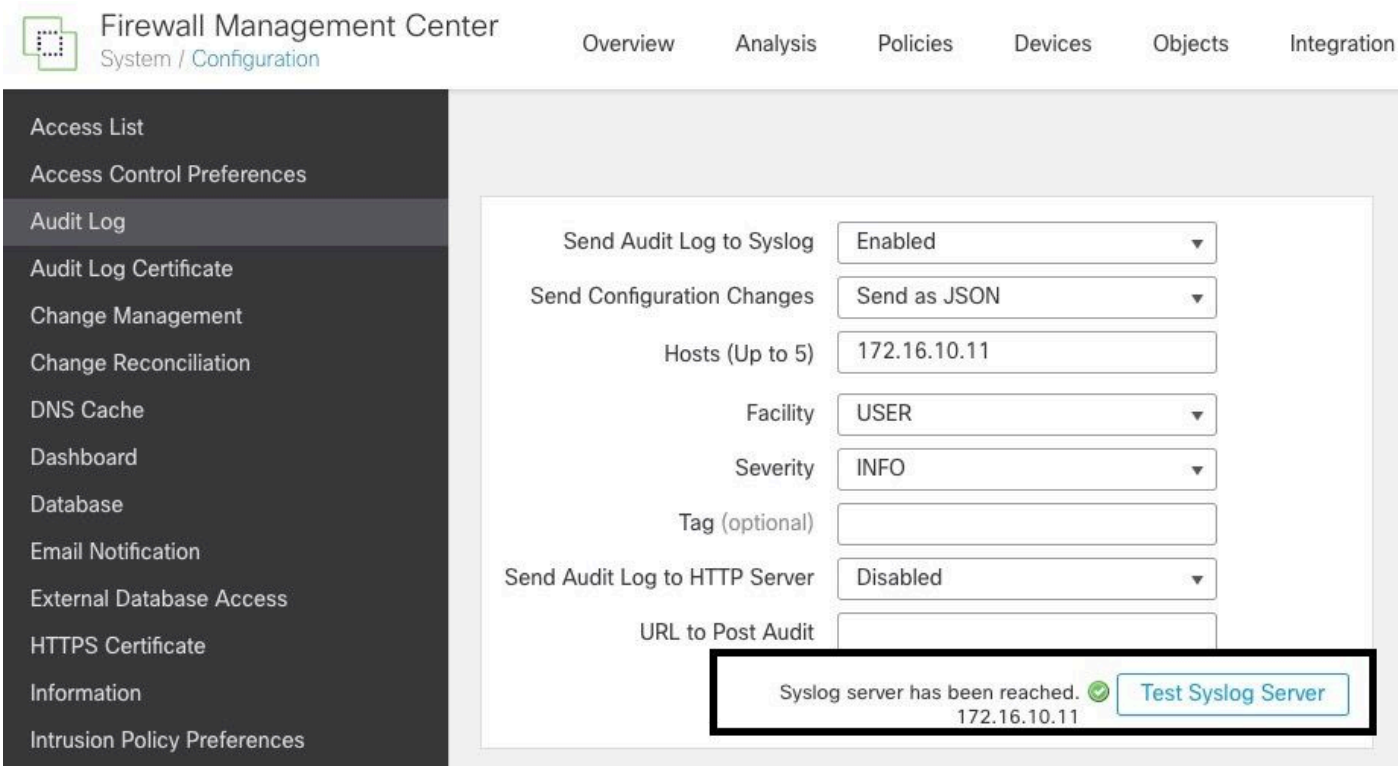
Dieses Bild zeigt die Parameter für die Konfiguration des Syslog-Servers für Audit-Protokolle:



Überprüfung

Um zu überprüfen, ob die Parameter richtig konfiguriert sind, wählen Sie System > Configuration > Audit Log > Test Syslog Server aus.

Dieses Bild zeigt einen erfolgreichen Syslog-Servertest:



Eine weitere Möglichkeit zur Überprüfung der Syslog-Funktionalität besteht darin, die Syslog-Schnittstelle zu überprüfen, um sicherzustellen, dass die Überwachungsprotokolle empfangen

werden.

Dieses Bild zeigt einige Beispiele der Überwachungsprotokolle, die vom Syslog-Server empfangen wurden:

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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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] 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
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] sftunneld: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] sftunneld: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"]SeshatI[10441]: 16959378200.8611.8214.3110.94[7814.9214815.2210.0080.0014.79]1.60[142.3980800.0080.0080080.0280.0680825580.0080.0080680.0210.0480816123.980.080.0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]EventdI[10442]: 1695937820[2112211750080
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"]SeshatI[10441]: 16959378101.0286.7332.5811.92110021.9086635.9080.0080.0811.71]1.60[367.2015827080.0080.0080080.0380.0580825580.0080.0080680.0480.0480816193.582.180.0
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]EventdI[10442]: 1695933781[0]212211175080
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"]SeshatI[10441]: 16959378000.5382.4611.3110.8617731.6750066.8110.0080.0085.1810.0076.41]1582860.0080.0080080.0380.0480825580.0080.0080680.0380.0380816107.411.480.0
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]EventdI[10442]: 1695933780[0]212211175080
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

Nachfolgend finden Sie einige Beispiele für Konfigurationsänderungen, die Sie in Ihrem Syslog-Server erhalten können:

```
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:
```

Fehlerbehebung

Nachdem die Konfiguration angewendet wurde, stellen Sie sicher, dass das FMC mit dem Syslog-Server kommunizieren kann.

Das System verwendet ICMP/ARP- und TCP SYN-Pakete, um sicherzustellen, dass der Syslog-Server erreichbar ist. Anschließend verwendet das System standardmäßig den Port 514/UDP zum Streamen von Audit-Protokollen und den TCP-Port 1470, wenn Sie den Kanal sichern.

Um eine Paketerfassung auf dem FMC zu konfigurieren, wenden Sie die folgenden Befehle an:

- tcpdump. Dieser Befehl erfasst den Datenverkehr im Netzwerk.

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

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

Um die ICMP-Erreichbarkeit zu testen, verwenden Sie zusätzlich den folgenden Befehl:

- Ping Mit diesem Befehl können Sie überprüfen, ob ein Gerät erreichbar ist, und die Latenz der Verbindung ermitteln.

```
> 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
```

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme
- Administratorleitfaden für Cisco Secure Firewall Management Center

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.