تكوين FMC لإرسال سجلات التدقيق إلى خادم syslog

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين سجلات تدقيق مركز إدارة جدار الحماية الآمن المراد إرسالها إلى خادم syslog.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الاستخدام الأساسي لمركز إدارة جدار الحماية (FMC) من Cisco
- فهم بروتوكول syslog

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Firewall Management Center Virtual v7.4.0
- خادم Syslog للجهة الخارجية

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يقوم "مركز إدارة جدار الحماية الآمن" بتسجيل نشاط المستخدم في سجلات التدقيق للقراءة فقط. عند بدء تشغيل Firepower الإصدار 7.4.0، يمكنك تدفق تغييرات التكوين كجزء من بيانات سجل التدقيق إلى syslog من خلال تحديد تنسيق بيانات التكوين والأجهزة المضيفة. يتيح لك تدفق سجلات التدقيق إلى خادم خارجي توفير مساحة على مركز الإدارة، كذلك، يكون مفيدا عندما تحتاج إلى توفير سجل تدقيق لتغييرات التكوين.

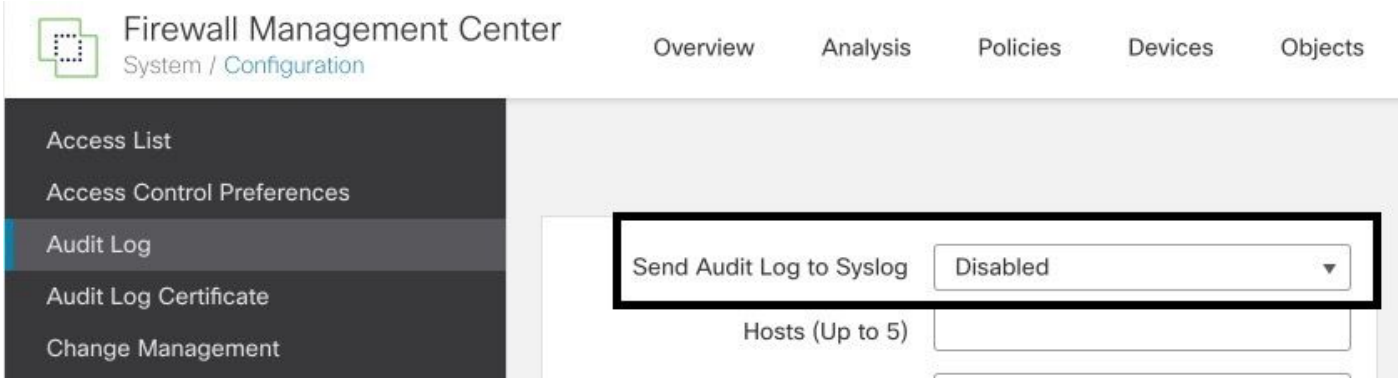
في حالة التوفر العالي، يتم توفير مركز إدارة لإرسال تغييرات التكوين syslog إلى خوادم syslog الخارجية. تتم مزامنة ملف السجل بين أزواج HA بحيث يكون في أثناء تجاوز الفشل أو التحويل، مركز إدارة سيستأنف إرسال سجلات التغيير. في حال كان زوج HA يعمل في نمط النقسام الدماغ، كل امركز إدارة يرسل ٪s في الزوج syslog تغيير التكوين إلى الخوادم الخارجية.

التكوين

الخطوة 1. سجلات التدقيق الممكنة إلى syslog

للتمكين لذلك يرسل FMC سجلات تدقيق إلى خادم syslog، انتقل إلى نظام > تشكيل > سجل تدقيق > إرسال سجل تدقيق إلى syslog > ممكن.

توضح هذه الصورة كيفية تمكين ميزة إرسال سجل التدقيق إلى syslog:



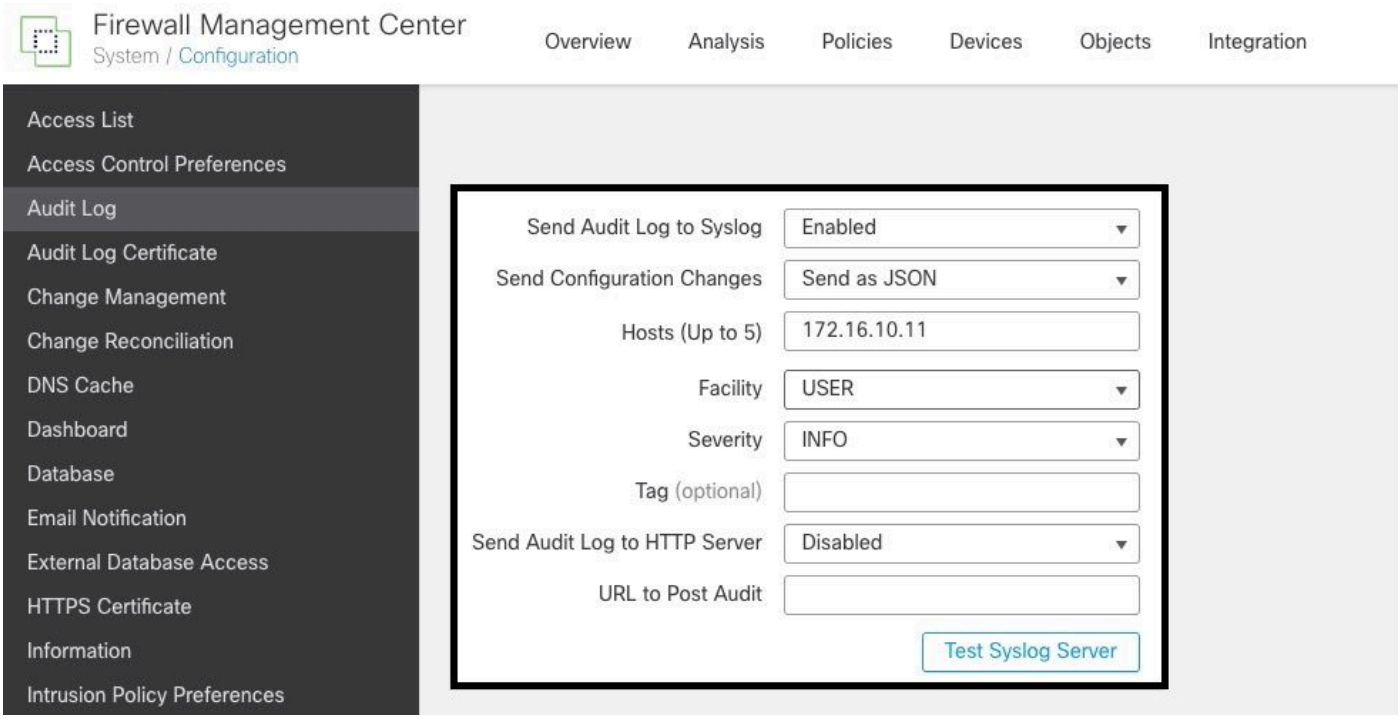
يمكن أن تدفق FMC بيانات سجل التدقيق إلى خمسة خوادم syslog كحد أقصى.

الخطوة 2. تكوين معلومات syslog

بعد تمكين الخدمة، يمكنك تكوين معلومات syslog. لتكوين معلومات syslog، انتقل إلى نظام > تكوين > سجل التدقيق.

وفقا لمتطلباتك، حدد إرسال تغييرات التكوين والمضيفين والمنشآت والخطوة

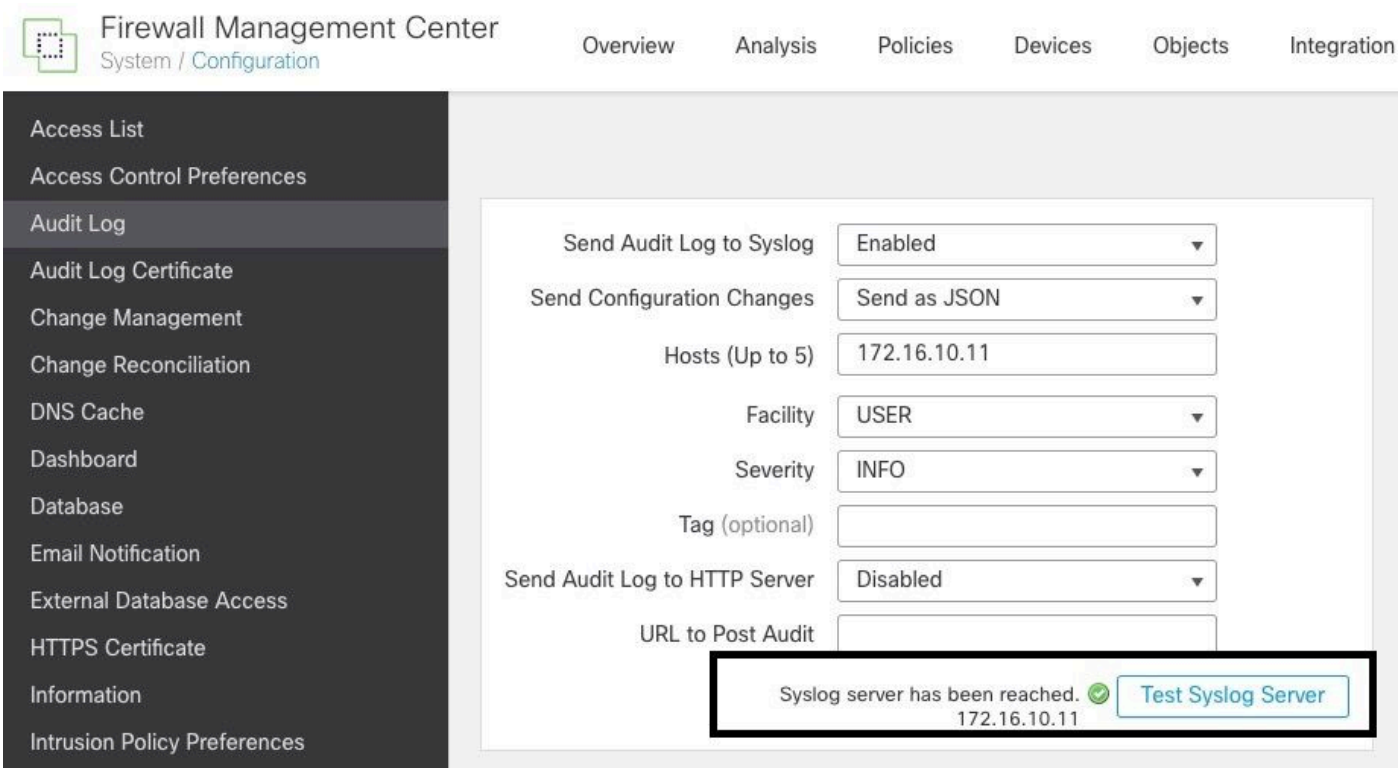
تعرض هذه الصورة المعلمات لتكوين خادم syslog لسجلات التدقيق:



التحقق من الصحة

للتحقق من تكوين المعلمات بشكل صحيح، حدد النظام > التكوين > سجل التدقيق > إختبار خادم syslog.

تعرض هذه الصورة إختبار خادم syslog بنجاح:



طريقة أخرى للتحقق من أن syslog يعمل، تحقق من واجهة syslog لتأكيد إستلام سجلات التدقيق.

تعرض هذه الصورة بعض الأمثلة على سجلات التدقيق التي تم استقبالها بواسطة خادم 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 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"]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
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]Eventds[10442]: 1695937820|2|122|1175|0|60
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]: 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
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]Eventds[10442]: 1695937810|2|122|1175|0|0
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]: 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
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]Eventds[10442]: 1695937800|2|122|1175|0|0
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

فيما يلي بعض الأمثلة على تغييرات التكوين التي يمكنك تلقيها في خادم 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:
```

استكشاف الأخطاء وإصلاحها

بعد تطبيق التكوين، تأكد من إمكانية اتصال FMC بخادم syslog.

يستخدم النظام حزم ICMP/ARP و TCP syn للتحقق من إمكانية الوصول إلى خادم syslog. بعد ذلك، يستخدم النظام بشكل افتراضي المنفذ 514/UDP لتدفق سجلات التدقيق ومنفذ TCP 1470 إذا قمت بتأمين القناة.

لتكوين التقاط حزمة على FMC، قم بتطبيق الأوامر التالية:

- tcpdump. على قبض هذا أمر الحركة مرور على الشبكة

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

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

وبالإضافة إلى ذلك، لاختبار إمكانية الوصول إلى ICMP، قم بتطبيق هذا الأمر:

- بينج. يساعد هذا الأمر في التأكد من إمكانية الوصول إلى جهاز ما أو عدم الوصول ومعرفة زمن الوصول إلى الاتصال.

```
> 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
```

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- دليل إدارة مركز إدارة جدار الحماية الآمن من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).