Configurer FMC pour envoyer les journaux d'audit à un serveur Syslog

Table des matières

Introduction

Ce document décrit comment configurer les journaux d'audit du Centre de gestion du pare-feu sécurisé à envoyer à un serveur Syslog.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Facilité d'utilisation de base de Cisco Firewall Management Center (FMC)
- Présentation du protocole Syslog

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firewall Management Center Virtual v7.4.0
- Serveur Syslog tiers

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le Centre de gestion du pare-feu sécurisé enregistre l'activité des utilisateurs dans des journaux d'audit en lecture seule. À partir de la version 7.4.0 de Firepower, vous pouvez transmettre les modifications de configuration dans le cadre des données du journal d'audit à syslog en spécifiant le format des données de configuration et les hôtes. La diffusion en continu des journaux d'audit vers un serveur externe vous permet de conserver de l'espace sur le centre de gestion. Elle est également utile lorsque vous devez fournir une piste d'audit des modifications de configuration.

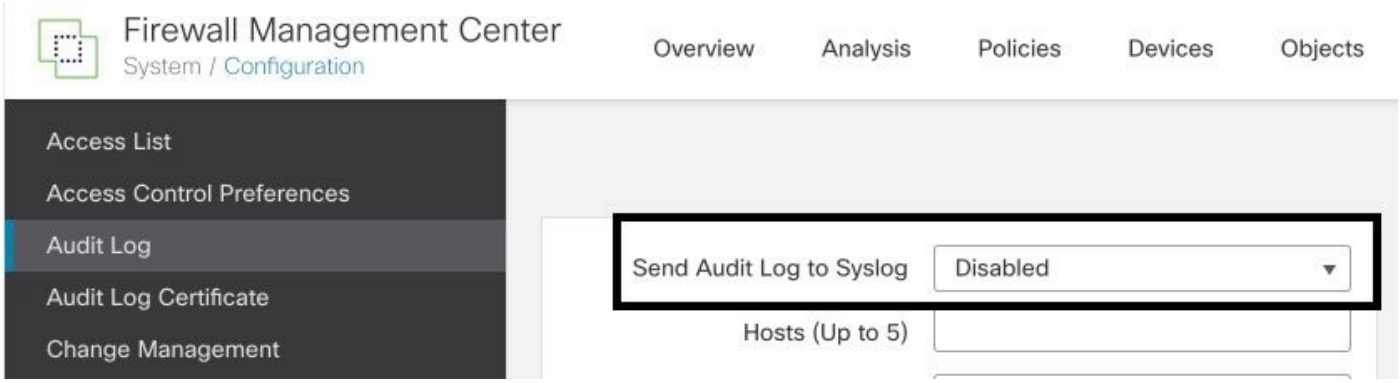
En cas de haute disponibilité, seul le centre de gestion envoie les modifications de configuration syslog aux serveurs syslog externes. Le fichier journal est synchronisé entre les paires haute disponibilité de sorte que lors d'un basculement ou d'une commutation, le nouveau centre de gestion reprendrait l'envoi des journaux des modifications. Si la paire HA fonctionne en mode « split-brain », les deux centre de gestions dans la paire envoie le syslog config change aux serveurs externes.

Configurer

Étape 1. Journaux d'audit activés dans Syslog

Pour activer l'envoi par FMC des journaux d'audit à un serveur Syslog, accédez à System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled.

Cette image montre comment activer la fonctionnalité Envoyer le journal d'audit vers Syslog :



Le FMC peut transmettre les données du journal d'audit à un maximum de cinq serveurs Syslog.

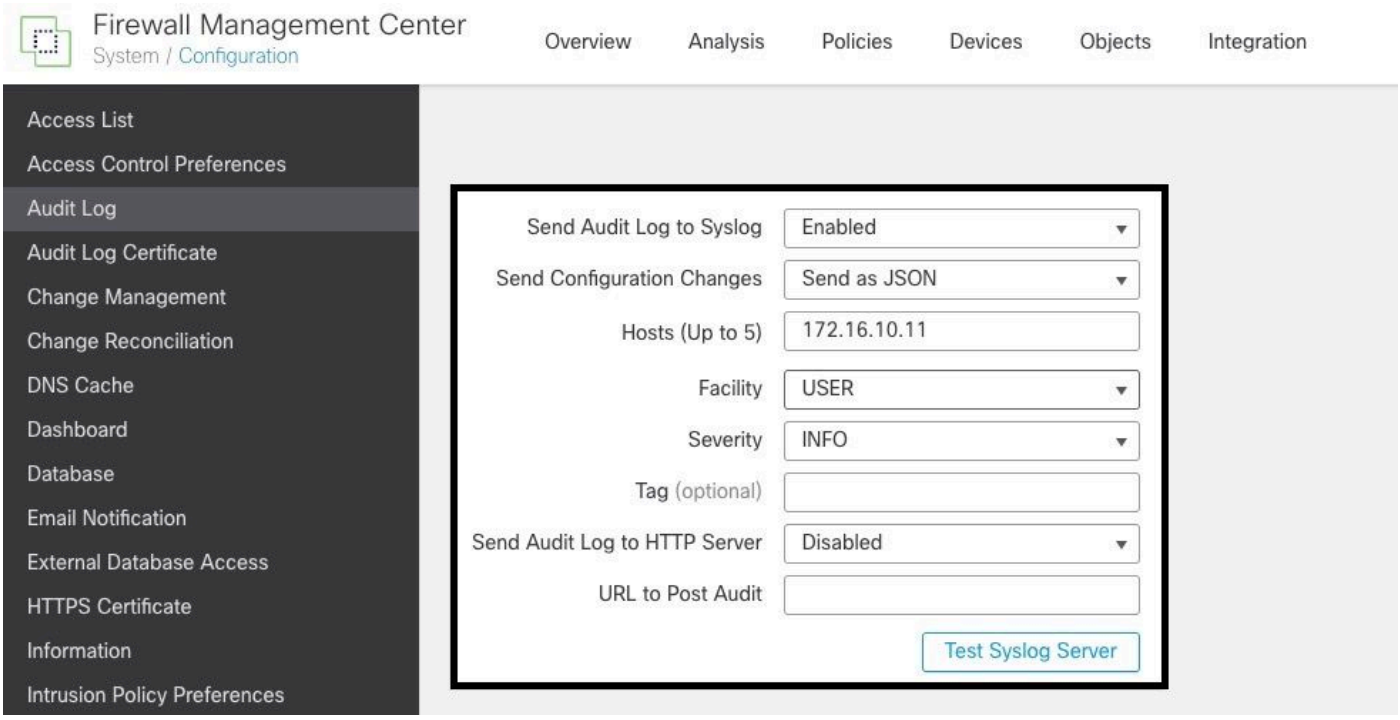
Étape 2. Configuration des informations Syslog

Une fois le service activé, vous pouvez configurer les informations Syslog. Pour configurer les informations Syslog, accédez à System > Configuration > Audit Log.

En fonction de vos besoins, sélectionnez Envoyer les modifications de configuration, Hôtes, Facilité, Gravité

Cette image présente les paramètres de configuration du serveur Syslog pour les journaux d'audit

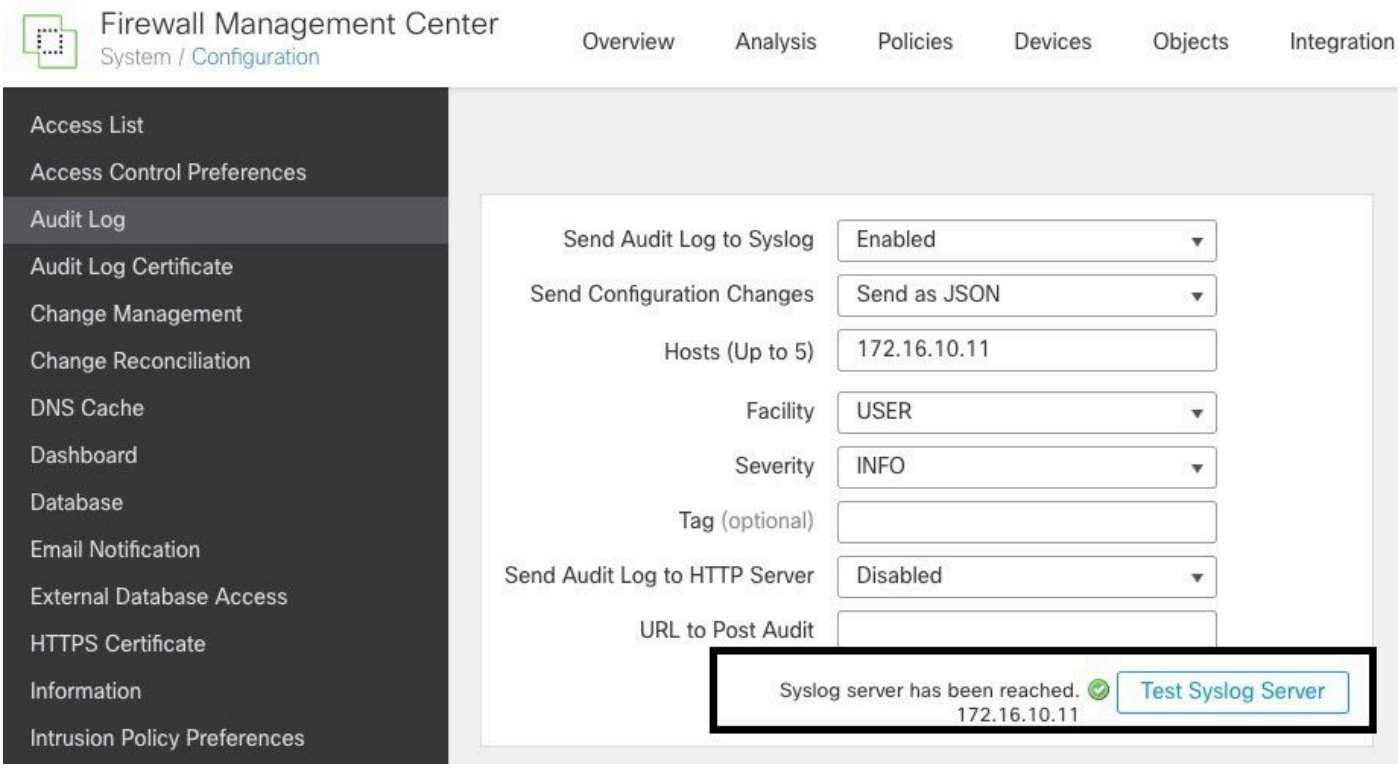
:



Vérifier

Pour vérifier si les paramètres sont correctement configurés, sélectionnez System > Configuration > Audit Log > Test Syslog Server.

Cette image montre un test réussi du serveur Syslog :



Une autre façon de vérifier que Syslog fonctionne, vérifiez l'interface Syslog pour confirmer que

les journaux d'audit sont reçus.

Cette image présente quelques exemples de journaux d'audit reçus par le serveur 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]: 16959378200.861.8214.3110.94(7814.9214815.220.0080.0014.79|1.60|142.3980800.0080.0080080.0280.0680825680.0080.0080680.0210.0400161623.980.080.0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]Eventds[10442]: 1695937820|2|1221175080|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"]SeshatI10441]: 16959378101.0295.73|32.5811.92110021.9086635.9080.0080.00111.71|1.60|367.2081527080.0080.0080080.0380.0580825580.0080.0080680.0480.0480161193.582.180.0
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]Eventds[10442]: 1695937810|2|1221175080
09-28-2023	21:49:58	User.Info	172.16.10.2	Sep 28 21:50:03 firepower: platformSettingsEdit.cgi: admin@10.152.201.95, System > Configuration > Configuration > /platinum/platformSettingsEdit.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"]SeshatI10441]: 16959378000.592.46|11.3110.86|7731.675066.8110.0080.0085.1810.00|76.41|1528680.0080.0080080.0380.0480825580.0080.0080680.0380.0380161107.411.480.0
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]Eventds[10442]: 1695937800|2|1221175080
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

Voici quelques exemples des modifications de configuration que vous pouvez recevoir sur votre serveur 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:
```

Dépannage

Une fois la configuration appliquée, assurez-vous que le FMC peut communiquer avec le serveur syslog.

Le système utilise des paquets ICMP/ARP et TCP SYN pour vérifier que le serveur Syslog est accessible. Ensuite, le système utilise par défaut le port 514/UDP pour diffuser les journaux d'audit et le port TCP 1470 si vous sécurisez le canal.

Pour configurer une capture de paquets sur FMC, appliquez ces commandes :

- tcpdump. Cette commande capture le trafic sur le réseau

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

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

En outre, pour tester l'accessibilité ICMP, appliquez cette commande :

- ping. Cette commande permet de confirmer si un périphérique est accessible ou non et de connaître la latence de la connexion.

```
> 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
```

Informations connexes

- Assistance et documentation techniques - Cisco Systems
- Guide d'administration de Cisco Secure Firewall Management Center

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.