Configurare FMC per l'invio di registri di controllo a un server Syslog

Sommario

Introduzione

In questo documento viene descritto come configurare i log di controllo di Centro gestione firewall protetti da inviare a un server Syslog.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Usabilità di base di Cisco Firewall Management Center (FMC)
- Informazioni sul protocollo Syslog

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firewall Management Center Virtual v7.4.0
- Server syslog di terze parti

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Centro gestione firewall protetto registra le attività degli utenti in registri di controllo di sola lettura. A partire dalla versione 7.4.0 di Firepower, è possibile trasmettere le modifiche alla configurazione come parte dei dati del log di controllo a syslog specificando il formato dei dati di configurazione e gli host. Lo streaming dei registri di verifica su un server esterno consente di preservare spazio nel centro di gestione ed è utile quando è necessario fornire un audit trail delle modifiche alla configurazione.

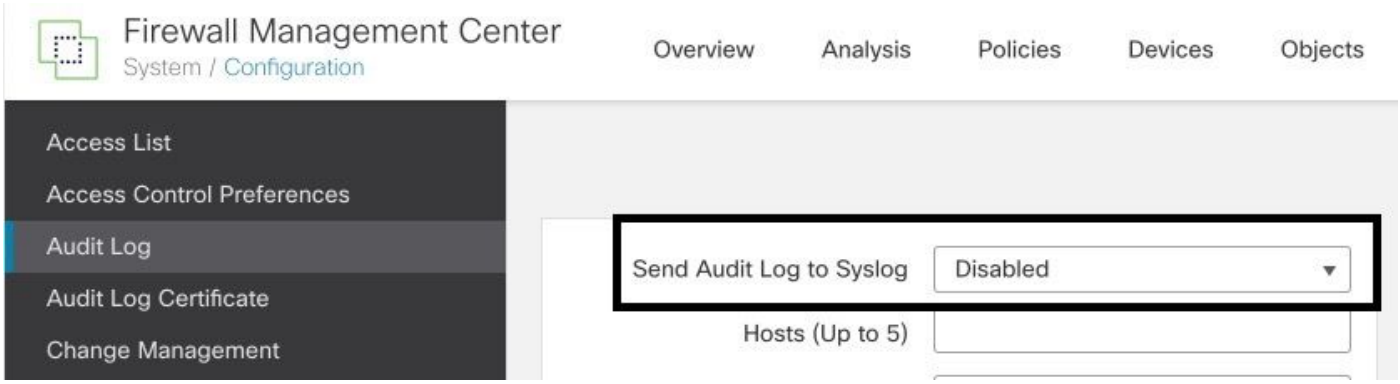
In caso di elevata disponibilità, solo il server attivo centro di gestione invia il syslog delle modifiche alla configurazione ai server syslog esterni. Il file di log viene sincronizzato tra le coppie HA in modo che, durante un failover o un passaggio, il nuovo centro di gestione riprende l'invio dei log delle modifiche. Nel caso in cui la coppia HA funzioni in modalità split-brain, entrambi centro di gestiones nella coppia invia il syslog di modifica della configurazione ai server esterni.

Configurazione

Passaggio 1. Registri di controllo abilitati per Syslog

Per attivare l'invio dei log di controllo da parte di CCP a un server syslog, selezionare Sistema > Configurazione > Log di controllo > Invia log di controllo a syslog > Abilitato.

Nell'immagine viene mostrato come abilitare la funzione Invia registro di controllo a syslog:



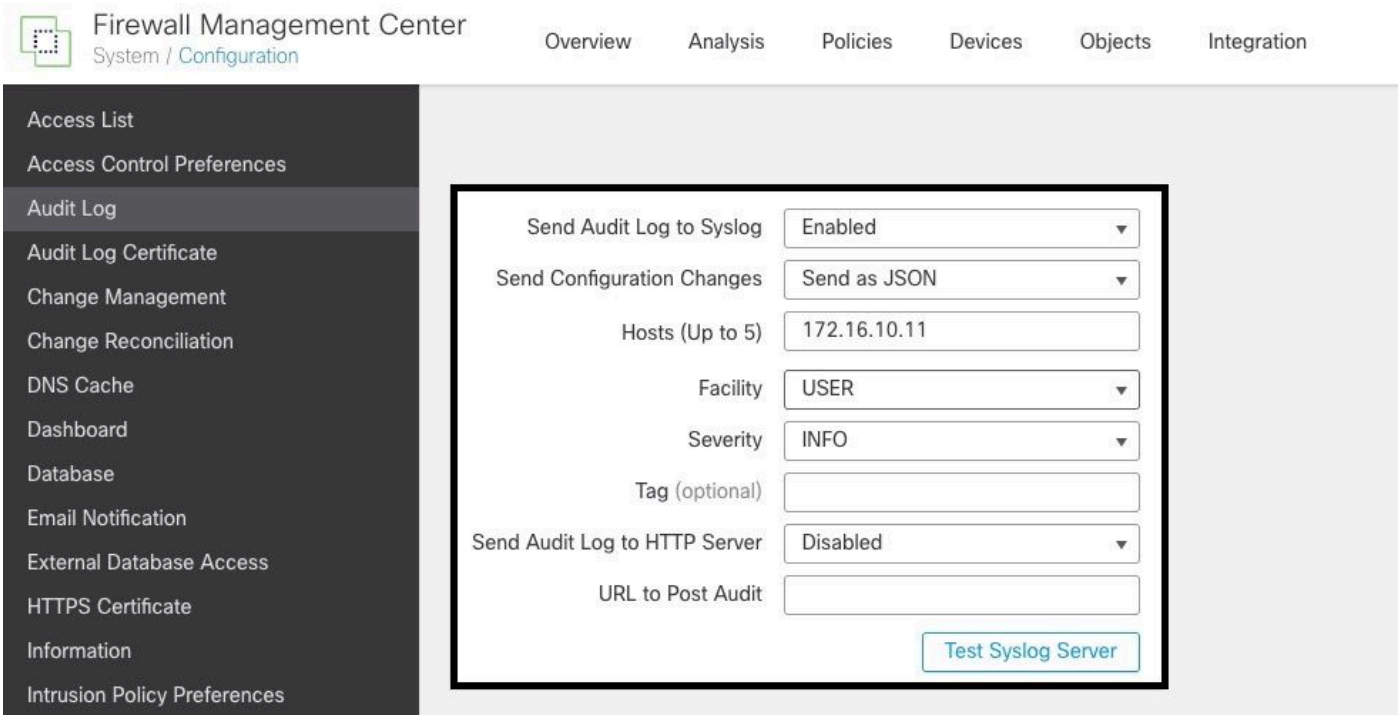
Il FMC può inviare i dati del registro di controllo a un massimo di cinque server syslog.

Passaggio 2. Configura informazioni syslog

Dopo aver abilitato il servizio, è possibile configurare le informazioni syslog. Per configurare le informazioni di syslog, selezionare Sistema > Configurazione > Registro di controllo.

In base alle esigenze, selezionare Send Configuration Changes, Hosts, Facility, Severity

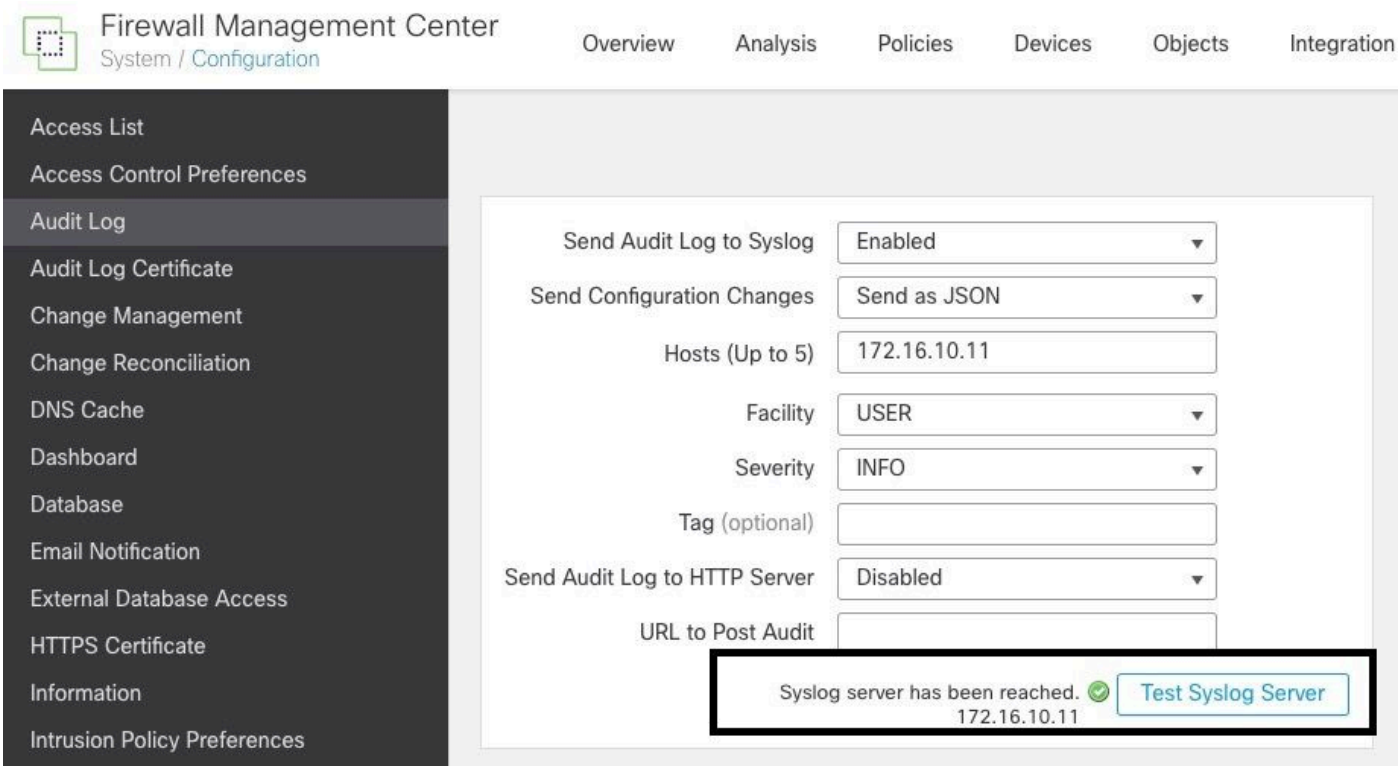
Nell'immagine sono illustrati i parametri per configurare Syslog Server per i log di controllo:



Verifica

Per verificare se i parametri sono configurati correttamente, selezionare Sistema > Configurazione > Registro di controllo > Test Syslog Server.

Nell'immagine viene mostrato un test del server Syslog riuscito:



Per verificare che syslog funzioni correttamente, controllare l'interfaccia syslog per verificare che i log di controllo siano stati ricevuti.

Nell'immagine sono illustrati alcuni esempi di log di controllo ricevuti dal server 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] 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]: 16959378200.861.8214.3110.947814.9214815.220.0000.0014.791.60142.3980800.0000.0000800.0200.0600255800.0000.0000600.0200.0400161623.980.000.0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequenceId="1911"]EventdJ[10442]: 1695937820212211750860
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"]SeshatJ[10441]: 16959378101.0296.73032.5801.92110021.9086635.9080.0000.00011.7111.60367.2001527080.0000.0000080.0300.0500255800.0000.0000600.0400.0400161193.582.100.0
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequenceId="1908"]EventdJ[10442]: 1695937810212211750080
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"]SeshatJ[10441]: 16959378000.5982.46011.3110.8627731.6775066.8110.0000.0005.1810.00076.4111528680.0000.0000080.0300.0400255800.0000.0000600.0300.0300161107.401.400.0
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequenceId="1901"]EventdJ[10442]: 1695937800212211750080
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

Di seguito sono riportati alcuni esempi delle modifiche alla configurazione che è possibile ricevere nel server 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:
```

Risoluzione dei problemi

Dopo aver applicato la configurazione, verificare che il CCP sia in grado di comunicare con il server syslog.

Il sistema utilizza i pacchetti ICMP/ARP e TCP SYN per verificare che il server syslog sia raggiungibile. Quindi, per impostazione predefinita, il sistema utilizza la porta 514/UDP per i log di controllo in streaming e la porta TCP 1470 se si protegge il canale.

Per configurare l'acquisizione di un pacchetto in FMC, applicare i seguenti comandi:

- tcpdump. Questo comando acquisisce il traffico sulla rete

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

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

Inoltre, per verificare la raggiungibilità del protocollo ICMP, applicare questo comando:

- ping Questo comando consente di verificare se un dispositivo è raggiungibile o meno e di conoscere la latenza della connessione.

```
> 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
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- Guida all'amministrazione di Cisco Secure Firewall Management Center

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).