

# 配置FMC以將稽核日誌傳送到系統日誌伺服器

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟 1.啟用到系統日誌的稽核日誌](#)

[步驟 2.配置系統日誌資訊](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔介紹如何配置要傳送到系統日誌伺服器的Secure Firewall Management Center稽核日誌。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 思科防火牆管理中心(FMC)的基本可用性
- 瞭解系統日誌協定

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科防火牆管理中心虛擬v7.4.0
- 第三方系統日誌伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Secure Firewall Management Center在只讀稽核日誌中記錄使用者活動。從Firepower 7.4.0版開始，可以通過指定配置資料格式和主機，將配置更改作為稽核日誌資料的一部分流式傳輸到系統日誌

。通過將稽核日誌流式傳輸到外部伺服器，可以節省管理中心上的空間，在需要提供配置更改的稽核跟蹤時，此功能也非常有用。

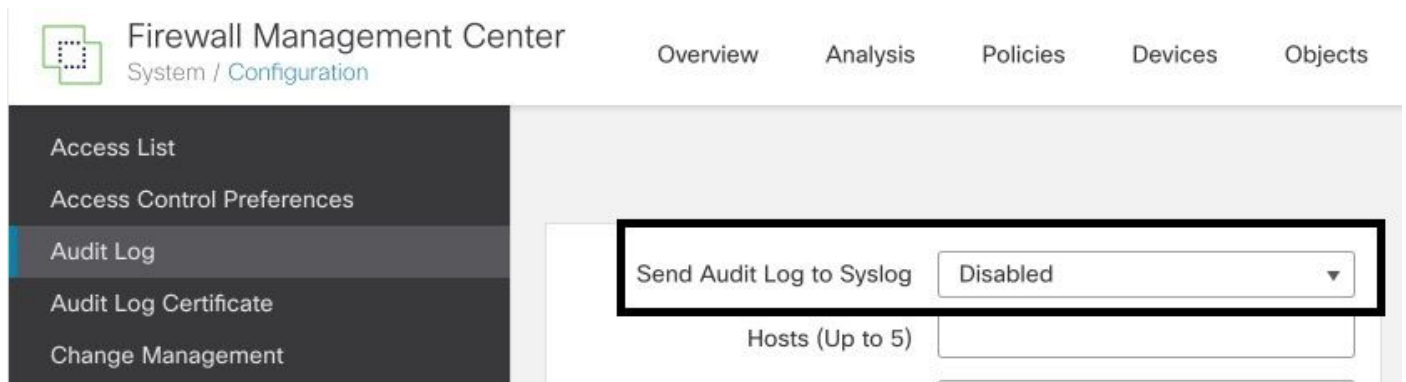
在高可用性情況下，只有活動 管理中心 將配置更改syslog傳送到外部syslog伺服器。日誌檔案在HA對之間同步，以便在故障切換或切換期間，新的主用日誌檔案將處於活動狀態 管理中心 繼續傳送更改日誌。如果HA對以大腦分割模式工作，則 管理中心對中的將配置更改系統日誌傳送到外部伺服器。

## 設定

### 步驟 1.啟用到系統日誌的稽核日誌

要啟用FMC將稽核日誌傳送到系統日誌伺服器，請導航到System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled。

此圖顯示如何啟用將稽核日誌傳送到系統日誌功能：



FMC最多可將審計日誌資料流式傳輸到五台系統日誌伺服器。

### 步驟 2.配置系統日誌資訊

啟用服務後，您可以配置系統日誌資訊。要配置系統日誌資訊，請導航到System > Configuration > Audit Log。

根據您的要求，選擇Send Configuration Changes， Hosts， Facility， Severity

此圖顯示配置用於稽核日誌的系統日誌伺服器的引數：

Firewall Management Center  
System / Configuration

Overview Analysis Policies Devices Objects Integration

Access List  
Access Control Preferences  
Audit Log  
Audit Log Certificate  
Change Management  
Change Reconciliation  
DNS Cache  
Dashboard  
Database  
Email Notification  
External Database Access  
HTTPS Certificate  
Information  
Intrusion Policy Preferences

Send Audit Log to Syslog Enabled  
Send Configuration Changes Send as JSON  
Hosts (Up to 5) 172.16.10.11  
Facility USER  
Severity INFO  
Tag (optional)  
Send Audit Log to HTTP Server Disabled  
URL to Post Audit  
Test Syslog Server

## 驗證

要驗證引數是否配置正確，請選擇System > Configuration > Audit Log > Test Syslog Server。


此圖顯示了成功的Syslog伺服器測試：

Firewall Management Center  
System / Configuration

Overview Analysis Policies Devices Objects Integration

Access List  
Access Control Preferences  
Audit Log  
Audit Log Certificate  
Change Management  
Change Reconciliation  
DNS Cache  
Dashboard  
Database  
Email Notification  
External Database Access  
HTTPS Certificate  
Information  
Intrusion Policy Preferences

Send Audit Log to Syslog Enabled  
Send Configuration Changes Send as JSON  
Hosts (Up to 5) 172.16.10.11  
Facility USER  
Severity INFO  
Tag (optional)  
Send Audit Log to HTTP Server Disabled  
URL to Post Audit

Syslog server has been reached.  Test Syslog Server  
172.16.10.11

另一種驗證系統日誌是否正常工作的方法是，檢查系統日誌介面以確認是否收到稽核日誌。

此圖顯示Syslog伺服器接收的審計日誌的一些示例：

Date	Time	Priority	Hostname	Message
09-28-2023	21:50:16	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1933"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1932"[19129] streamfile [INFO] AFTER FOUND COMPL TASK ON SRC: cur_read=40, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1931"[19129] streamfile [INFO] FILE /var/ssl/idsm_download/7cb124a4-4c0e-11ee-b245-a2990c0ac7a0
09-28-2023	21:50:16	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1930"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1929"[19129] streamfile [INFO] ADDED INIT confirmation to be SRC: cur_read=0, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1928"[19129] streamfile [INFO] Adding SRC Task on Request, key: 0.204
09-28-2023	21:50:16	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1927"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1926"[19129] streamfile [INFO] Creating task on SRC for incoming task: cur_read=0, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1925"[19129] streamfile [INFO] SRC TASK for KEY 0.204 was not found
09-28-2023	21:50:16	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequencelid="1924"[19129] streamfile [INFO] ELASTIC/STREAM request DoNotBlockList validation passed for: /var/ssl/idsm_download/7cb124a4-4c0e-11ee-b245-a2990c0ac7a0
09-28-2023	21:50:16	Local/Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[9765]: [meta sequencelid="1923"[19129] streamfile [INFO] Sending message at /usr/local/sbin/jpent/5.32.1/SF/HealthMon.pm line 579.
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1922"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1921"[19129] streamfile [INFO] AFTER FOUND COMPL TASK ON SRC: cur_read=42, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1920"[19129] streamfile [INFO] FILE /var/ssl/idsm_download/7cb2fa4a-4c0e-11ee-b245-a2990c0ac7a0
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1919"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1918"[19129] streamfile [INFO] ADDED INIT confirmation to be SRC: cur_read=0, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1917"[19129] streamfile [INFO] Adding SRC Task on Request, key: 0.202
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1916"[19129] streamfile [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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1915"[19129] streamfile [INFO] Creating task on SRC for incoming task: cur_read=0, cur_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	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1914"[19129] streamfile [INFO] SRC TASK for KEY 0.202 was not found
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequencelid="1913"[19129] streamfile [INFO] ELASTIC/STREAM request DoNotBlockList validation passed for: /var/ssl/idsm_download/7cb2fa4a-4c0e-11ee-b245-a2990c0ac7a0
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequencelid="1912"[19129] streamfile [INFO] 16959378200.861.824.310.947014.924815.220.000.004.791.60142.390000.000.000000.020.06002550.000.000060.020.04001623.300.00.0
09-28-2023	21:50:15	Local/Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]: [meta sequencelid="1911"[19129] streamfile [INFO] 16959378200.861.824.310.947014.924815.220.000.004.791.60142.390000.000.000000.020.06002550.000.000060.020.04001623.300.00.0
09-28-2023	21:50:07	Local/Debug	172.16.10.2	Sep 28 21:50:12 firepower SF-IMS[9765]: [meta sequencelid="1910"[19129] streamfile [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:50:05	Local/Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequencelid="1909"[19129] streamfile [INFO] 16959378101.026.7332.5081.9210021.908635.9080.0000011.7111.60067.201522700.000.000080.030.04002550.000.000060.030.030016107.411.400.0
09-28-2023	21:50:05	Local/Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]: [meta sequencelid="1908"[19129] streamfile [INFO] 16959378101.026.7332.5081.9210021.908635.9080.0000011.7111.60067.201522700.000.000080.030.04002550.000.000060.030.030016107.411.400.0
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 > /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@0efaa0 User IP, Login, Login Success
09-28-2023	21:49:57	Local/Debug	172.16.10.2	Sep 28 21:50:02 firepower SF-IMS[9765]: [meta sequencelid="1907"[19129] streamfile [INFO] sshd is running with 2046 4005 3992 2046
09-28-2023	21:49:57	Local/Debug	172.16.10.2	Sep 28 21:50:02 firepower store_allowlist_history: [meta sequencelid="1906"[19129] streamfile [INFO] store_allowlist_history finished successfully.
09-28-2023	21:49:56	Local/Debug	172.16.10.2	Sep 28 21:50:01 firepower store_allowlist_history: [meta sequencelid="1905"[19129] streamfile [INFO] invoking /usr/local/sbin/store_allowlist_history.pl
09-28-2023	21:49:56	Local/Debug	172.16.10.2	Sep 28 21:50:01 firepower CROND[6894]: [meta sequencelid="1904"[19129] streamfile [INFO] CMD (/usr/libexec/aa/aal 1 1)
09-28-2023	21:49:56	Local/Debug	172.16.10.2	Sep 28 21:50:01 firepower CROND[6893]: [meta sequencelid="1903"[19129] streamfile [INFO] CMD (/usr/local/sbin/rum-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	Local/Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequencelid="1902"[19129] streamfile [INFO] 16959378000.592.4611.310.867731.675066.810.000.005.180.00076.411152860.000.000000.030.04002550.000.000060.030.030016107.411.400.0
09-28-2023	21:49:55	Local/Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS[9765]: [meta sequencelid="1901"[19129] streamfile [INFO] 16959378000.592.4611.310.867731.675066.810.000.005.180.00076.411152860.000.000000.030.04002550.000.000060.030.030016107.411.400.0
09-28-2023	21:49:52	User.Info	172.16.10.2	Sep 28 21:49:57 firepower audit_cst.cgi: admin@10.152.201.95, System > Configuration > Configuration > /admin/audit_cst.cgi, Page View

以下是可以在系統日誌伺服器中接收的配置更改的一些示例：

```

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:

```

## 疑難排解

應用配置後，確保FMC可以與syslog伺服器通訊。

系統使用ICMP/ARP和TCP SYN資料包驗證系統日誌伺服器是否可訪問。然後，如果保護通道，系統預設使用埠514/UDP傳輸審計日誌，使用TCP埠1470。

要在FMC上配置資料包捕獲，請應用以下命令：

- tcpdump.此命令可擷取網路上的流量

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/Volume/home/admin# tcpdump -i eth0 host 172.16.10.11 and port 514
```

此外，若要測試ICMP可達性，請應用以下命令：

- ping。此命令有助於確認裝置是否可訪問以及瞭解連線的延遲。

```
> 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
```

## 相關資訊

- [技術支援與文件 - Cisco Systems](#)
- [思科安全防火牆管理中心管理指南](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。