# 配置FMC以將稽核日誌傳送到系統日誌伺服器

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>步驟 1.啟用到系統日誌的稽核日誌</u> <u>步驟 2.配置系統日誌資訊</u> <u>驗證</u> <u>疑難排解</u> <u>相關資訊</u>

## 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志 。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:

Firewall Management Center System / Configuration	Overview	Analysis	Policies	Devices	Objects
Access List Access Control Preferences	3				
Audit Log Audit Log Certificate	Send Audit Log	g to Syslog	Disabled		•
Change Management	Host	s (Up to 5)			

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 A	Analysis	Policies	Devices	Objects	Integration
Access List						
Access Control Preferences						
Audit Log	Send Audit Log to	Syslog	Enabled			
Audit Log Certificate	ocha Addit Eog to	Cyslog [	Enabled		·	
Change Management	Send Configuration C	hanges	Send as JSO	N	•	
Change Reconciliation	Hosts (L	Jp to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard	S	Severity	INFO		•	
Database	Tag (a)	otional)				
Email Notification	Tag (0)					
External Database Access	Send Audit Log to HTTP	Server	Disabled		•	
HTTPS Certificate	URL to Pos	st Audit				
Information			[	Test Syslog	Server	
Intrusion Policy Preferences						

## 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	Send Audit Log t	to Svslog	Enabled		•	
Audit Log Certificate	oond Addit Log (	to bysing		5%	· _	
Change Management	Send Configuration	Changes	Send as JSO	N	•	
Change Reconciliation	Hosts	(Up to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard		Severity	INFO		¥	
Database	Tag (	optional)				
Email Notification						
External Database Access	Send Audit Log to HTT	P Server	Disabled		•	
HTTPS Certificate	URL to P	ost Audit				
Information		Syslog	server has been	n reached. 📀	Test Syslog	Server
Intrusion Policy Preferences			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	Isne	Priority	Hostname	Message
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [neta sequence[d="1933"][19129] strunneld:stream_life (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 5F-MST[10117]. Ineta sequenced="1322"[13123] thumeded stream A fiel INFO] AFTER FOUND COMPL TASK ON SRC: cur_read=40, cur_wite=40, total_bytes=40, theam_id_stc=0, thream_id_dest=204, seq_id_stc=1, task_distal_based and task_distal_based a
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]; [ineta sequenceld="1931"][19129] situmedd: stream_file [INFO] FILE /var/s1/sidns_download/7cb124a4-4c8e-11ee-b245-a2990cdac7a0
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 [irepower SF-IMS[10417]: [meta sequenceld="1930"][19129] situeneld: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 finepomes 5F WS100172 [inela sequenceId=1937][19173] situanedi stream_file [INF0] ADDED INIT confination to be SRC: cur_read=0, cur_wite=0, total_bytes=0, stream_id_strc=0, stream_id_strc=204, steg_id_strc=0, stream_id_strc=0, str
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]; [meta requence[d="1928"[[19129]] situmedd:steam_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 sequenceld="1927"][19129] situnneld: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 firepomes 5F145[10417] [incla sequenceid=19357[19172] itlnmedi stream_life [INF0] Creating task on SRC for incoming task: cur_read=0, cur_mite=0, total_bytes=0, stream_id_est=2004, seq_id_strc=0, seq_id_est=0 state=5stated, tasted 2023 09 28 21:2052 111(C, espine):2023 09 21 211C
03-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1925"][19129] situnneld:stream_life (INF0) SBC 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 sequenceld="1924"][19129] =thunneld:stream_file [INFO] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/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/s1/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-INS[10417]: [meta sequenceld="1922"][19129] situaneld:stream_life [INFO] AFTER FDUND 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 20:15:020 linepome 57:W5[10417] [inela sequenceid=1921*[]19123] it/menetit stream_life [INF0] AFTER FOUND COMPL TASK ON SRC: cur_tead=42, cur_wite=42, total_bytes=42, stream_id_tsc=0, stream_id_test=2022 rg 2022 vg 202
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 20 21:50:20 firepower SF-IMS[10417]: [ineta requenceId="1920"][19129] situaneld: stream_file (INFO) FILE /var/sf/sidn1_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 requence[d="1919"][19129] situaneld: Itream_file [INF0] 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 1:50.20 linepower 5F WS100172 [line1a sequenceld=19187][19172] situanedi stream_file [INF0] ADDED INIT confination to be SRC: cur_read=0, cur_wite=0, total_bytes=0, stream_id_usc=0, stre
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-INS[10417]: [ineta sequenceld="1917"][19129] situnneld: 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]: [ineta sequenceId="1916"][19129] situnneld: stream_life [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 [incposes 57:W5[10017] [incla sequenced1915"][19123] sthemetic stream_life [NFO] Enabling task on SRE for incoming task: cur_read-0, cur_mite-0, total_byter-0, stream_id_est-2022, seq_id_stc-0, seq_id_dest- state - Stated, tasted 2023 09 28:12562 2011C, explicit 2020 20 2011C
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta sequenceld="11914"][19129] sitrumeld:stream_file [INF0] 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]: [neta sequenceld="11913"][19129] situnneld:stream_life [INF0] ELASTIC/FSTREAM request DoNotBlockList validation passed for: /var/st/sidni_download/?cb2fa4a-4c0e-11ee-b245-a2990cdac?a0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[9765]; [meta sequenceId+"1912"]Seshal[10441]; 1695937820(0.06[1.82]4.31]0.94[7814.92]4815.22[0.00]0.00[0.00]4.79[1.60]142.39[0]00.02[0.00]00[0.02]0.06[0.02]50.00[0]00[0.02]0.04[0]6[2.39]0.00].
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]122111750060
09-28-2023	21:50:07	Local7.Debug	172.16.10.2	Sep 28 21:50:12 firepower SF-IMS(9765); [meta sequenceld="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 requenceld="1909"]Serihal[10441]; 1695937810[1.026; 73]32:50[1.92]10021.90(6535.90)0.0000.0011.71]1.60(367.2015)[270]0.0000.000000.0300.050(2550.00)0.00(006)0.040.040016(193.5)[2.10.0]
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 firepower SF-IMS[9765]; [meta sequenceId="1909"]Eventds[10442]; 1695937910[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 > /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: ActionQuevetScrape.pt. 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 sequenceld="1907"]szhd_monitor[9974]: szhd 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 sequenceld+"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_allowfirt_history: [meta sequenceId="1905"]Invoking '/usr/local/sif/bin/store_allowfirt_history.pf.
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 firepower CROND[6894]: [meta sequenceld="1904"][root] CMD (/usr/libexec/sa/sa1 1]
09-28-2023	21:49.56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 firepower CROND[6893]; [meta sequenceld="1903"](root) CMD ( /usr/local/s1/bin/um-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 sequence1d="1902"[Seshal[10441]; 169593700010.5912.46(11.31)0.86(7731.67)5666.8110.0010.000; 1810.00176.41(15128610.0010.0000000.0310.040(255)0.0000.0000000,0310.040(255)0.0000.0000000,0310.040(255)0.0000.0000000,0310.040(255)0.0000.0000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.00000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.000000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.0000.00000,0310.040(255)0.00000,0310.040(250)0000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,0300000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,0300000,0300000,0300000,030000,030000,0300000,030000,0300000,03000000
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS(9765); [meta sequenceld="1901")Eventds[10442]; 16959378000[2]122111751000
09-28-2023	21:49:52	Ilser Info	172 16 10 2	Sep 28.21-49-57 Gregomer: audit cert cei: admin@10.152.201.95 System > Configuration > Configu

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

- <u>技術支援與文件 Cisco Systems</u>
- 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)。