# 配置FMC以将审核日志发送到系统日志服务器

#### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>配置</u> <u>步骤1:启用到系统日志的审核日志</u> <u>第二步:配置系统日志信息</u> <u>验证</u> <u>故障排除</u> 相关信息

### 简介

本文档介绍如何配置要发送到系统日志服务器的Secure Firewall Management Center Audit Logs。

### 先决条件

#### 要求

Cisco 建议您了解以下主题:

- 思科防火墙管理中心(FMC)的基本可用性
- 了解系统日志协议

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科防火墙管理中心虚拟v7.4.0
- 第三方系统日志服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

#### 背景信息

安全防火墙管理中心在只读审核日志中记录用户活动。从Firepower版本7.4.0开始,可以通过指定 配置数据格式和主机,将配置更改作为审核日志数据的一部分流式传输到系统日志。通过将审核日 志流式传输到外部服务器,可以节省管理中心上的空间,当您需要提供配置更改的审核跟踪时,此 功能也非常有用。

在高可用性情况下,只有活动 管理中心 将配置更改syslog发送到外部系统日志服务器。日志文件在 HA对之间同步,以便在故障切换或切换期间,新的主用 管理中心 将会继续发送更改日志。如果 HA对以大脑分裂模式工作,则两者 管理中心对中的将配置更改系统日志发送到外部服务器。

### 配置

步骤1:启用到系统日志的审核日志

要启用FMC将审核日志发送到系统日志服务器,请导航到System > Configuration > Audit Log > Send Audit Log to Syslog > Enabled。

此图显示如何启用将审核日志发送到系统日志功能:

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

FMC最多可以将审核日志数据流式传输到五台系统日志服务器。

第二步:配置系统日志信息

启用服务后,您可以配置系统日志信息。要配置系统日志信息,请导航到System > Configuration > Audit Log。

根据您的要求,选择发送配置更改、主机、设施、严重性

此图显示用于配置审核日志的系统日志服务器的参数:

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	ochd Addit Eog to	Cyslog [	Enabled		·	
Change Management	Send Configuration C	hanges	Send as JSO	N	•	
Change Reconciliation	Hosts (U	Jp to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard	S	Severity	INFO		•	
Database	Tag	etional) [				
Email Notification	Tag (o)	ptional)				
External Database Access	Send Audit Log to HTTP	Server	Disabled		•	
HTTPS Certificate	URL to Pos	st Audit				
Information			ſ	Test Syslog	Server	
Intrusion Policy Preferences						

## 验证

要验证参数是否配置正确,请选择System > Configuration > Audit Log > Test Syslog Server。

#### 此图显示成功的Syslog服务器测试:

Access List Access Control Preferences	
Access Control Preferences	
Audit Log Send Audit Log to Syslog Enabled	Ţ
Audit Log Certificate	<u> </u>
Change Management Send Configuration Changes Send as JSON	•
Change Reconciliation Hosts (Up to 5) 172.16.10.11	
DNS Cache Facility USER	•
Dashboard Severity INFO	v
Database Tag (optional)	
Email Notification	
External Database Access	<b>v</b>
HTTPS Certificate URL to Post Audit	
Information Syslog server has been reached. Information	Syslog Server
Intrusion Policy Preferences	

另一种验证系统日志是否工作的方法,检查系统日志接口以确认是否收到审核日志。

下图显示了Syslog服务器接收的审计日志的一些示例:

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_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 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, theam_id_dest=204, seq_id_stc=1, task_distal_based and task_
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] situanceId stream_file [INF0] ADDED INIT confirmation to be SRC: cur_read=0, cur_wite=0, total_bytes=0, stream_id_strc=0, stream_id_strc=204, steg_id_stre=0, stream_id_stre=204, steg_id_stre=204,
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] [inela sequenceid=19357[19172] situanedi stream_lide [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; stated 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] sthunneld: 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/pen//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 requenceld="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] stannedic stream_life [NFO] [incating task on SRC 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, experiment2023 09 28 20:00 20 UTC
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-IMS[10417]: [meta 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[0255]0.00]0.00[0]0[0]0.02]0.04[0]16[23.9]0.00]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]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 requenceId="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)0.00000,0310.03000,0300000,030000,0300000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000,030000
09-28-2023	21:49:55	Local7.Debug	172.16.10.2	Sep 28 21:50:00 firepower SF-IMS(9765); [meta sequenceld="1901")Evenda;[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

以下是一些可在系统日志服务器中接收的配置更改示例:

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:

### 故障排除

应用配置后,确保FMC可以与syslog服务器通信。

系统使用ICMP/ARP和TCP SYN数据包验证系统日志服务器是否可访问。然后,如果您保护信道 ,系统默认使用端口514/UDP传输审核日志,使用TCP端口1470。

要在FMC上配置数据包捕获,请应用以下命令:

• tcpdump。此命令可捕获网络上的流量

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

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

#### 此外,要测试ICMP可达性,请应用以下命令:

• ping。此命令有助于确认设备是否可访问,并了解连接的延迟。

> 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

### 相关信息

- <u>技术支持和文档 Cisco Systems</u>
- 思科安全防火墙管理中心管理指南

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。