Syslogサーバに監査ログを送信するための FMCの設定

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 背景説明

 設定

 ステップ1: Syslogへの監査ログの有効化

 ステップ2: Syslog情報の設定

 確認

 トラブルシュート

 関連情報

概要

このドキュメントでは、Syslogサーバに送信されるSecure Firewall Management Center(SCM)監 査ログを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Cisco Firewall Management Center(FMC)の基本的な操作性
- Syslogプロトコルの理解

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firewall Management Center仮想v7.4.0
- ・ サードパーティのSyslogサーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

Secure Firewall Management Centerは、読み取り専用の監査ログにユーザアクティビティを記録 します。Firepowerバージョン7.4.0以降では、設定データのフォーマットとホストを指定するこ とで、監査ログデータの一部として設定変更をsyslogにストリームできます。外部サーバに監査 ログをストリーミングすることで、管理センターのスペースを節約できます。また、設定変更の 監査証跡を提供する必要がある場合にも役立ちます。

ハイアベイラビリティの場合は、アクティブな 管理センター 設定変更syslogを外部syslogサーバ に送信します。ログファイルはHAペア間で同期されるため、フェールオーバーまたはスイッチオ ーバーの際に新しいペアがアクティブになります 管理センター 変更ログの送信を再開します。 HAペアがスプリットブレインモードで動作している場合は、両方とも 管理センターペア内のは 、config change syslogを外部サーバに送信します。

設定

ステップ1:Syslogへの監査ログの有効化

FMCがsyslogサーバに監査ログを送信するようにするには、System > Configuration > Audit Log > Send Audit Log to Syslog > Enabledの順に移動します。

次の図に、Send Audit Log to Syslog機能を有効にする方法を示します。

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

FMCは、最大5台のsyslogサーバに監査ログデータをストリーミングできます。

ステップ 2: Syslog情報の設定

サービスを有効にした後で、syslog情報を設定できます。syslog情報を設定するには、System > Configuration > Audit Logの順に移動します。

要件に応じて、Send Configuration Changes, Hosts, Facility, Severityを選択します。

次の図に、監査ログ用にSyslogサーバを設定するパラメータを示します。

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	oond Addit Log to	cyolog [Enabled	<i>n</i> .		
Change Management	Send Configuration Cl	hanges	Send as JSON	1	•	
Change Reconciliation	Hosts (U	lp to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard	S	Severity	INFO		•	
Database	Tag (or	otional)				
Email Notification	149 (0)					
S External Database Access	end Audit Log to HTTP	Server	Disabled		•	
HTTPS Certificate	URL to Pos	st Audit				
Information			ſ	Test Syslog	Server	
Intrusion Policy Preferences						

確認

パラメータが正しく設定されているかどうかを確認するには、System > Configuration > Audit Log > Test Syslog Serverの順に選択します。

次の図は、成功したSyslogサーバテストを示しています。

Firewall Management Center System / Configuration	Overview	Analysis	Policies	Devices	Objects	Integration
Access List						
Access Control Preferences						
Audit Log	Send Audit Loo	a to Syslog	Enabled		•	
Audit Log Certificate	Cond / Iddit 200	, to eyeleg		55		
Change Management	Send Configuratio	n Changes	Send as JSO	N	•	
Change Reconciliation	Host	s (Up to 5)	172.16.10.11			
DNS Cache		Facility	USER		•	
Dashboard		Severity	INFO		•	
Database	Tac	(optional)	[
Email Notification						
External Database Access	end Audit Log to H	TTP Server	Disabled		•	
HTTPS Certificate	URL to	Post Audit				
Information		Syslog	g server has bee	n reached. 📀	Test Syslog	Server
Intrusion Policy Preferences		m	173	2.16.10.11		

syslogが機能していることを確認するもう1つの方法は、syslogインターフェイスをチェックして 監査ログが受信されていることを確認することです。

次の図に、Syslogサーバが受信する監査ログの例を示します。

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]: [ineta sequenceld="1933"][19129] situnneld: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 27:50.21 [incposer SF-IM5[1017] [neta sequence1d="1322"]19123] itbuneds iteam. (An UNTO) AFTER FOUND COMPL TASK ON SRC: cur_read=40, cur_wite=40, total_bytes=40, iteam_id_stc=-0, iteam_i
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 29 21:50:21 firepower SF-IMS[10417]: [meta sequenceld="1931"][19129] situnneld: stream_file [INF0] FILE /var/s1/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-INS[10417]: [meta sequenceId="11300"][19123] situmedd:stream_slile [INFO] ADDED INIT continuation 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 27:59.21 [freqperers 5F.M51[0417] [neta requenceds ⁴⁻¹⁹ 237 ¹ [13123] rthumself stream_file [INFO] ADDED INIT confirmation to be SRC: cur_read-0, cur_mite-0, total_bytes-0, stream_id_usc-0, stream_id_dest-204, seq_id_usc-0, stream_id_dest-204, seq_id_usc-0, stream_id_dest-204, seq_id_usc-0, stream_id_usc-0, stream_id_usc
09-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="11928"][19123] siftumeld: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 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 (Response SF-INST[0117]; Intent sequenceds ¹⁰ :1925 ¹¹ [1123] (Humsdichtman_file [INFO] Creating task on SRC for incoming task; cur_read-0, cur_mite-0, total_bytes=0, thream_id_usc=0, thream_id_usc=0, t
03-28-2023	21:50:16	Local7.Debug	172.16.10.2	Sep 28 21:50:21 firepower SF-IMS[10417]: [meta sequenceId="11925"][19129] situmetid:stream_tile [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 sequenceld="1924"][19129] sthunneld:stream_life [INFO] ELASTIC/FSTREAM request DeNotBlockList 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"jrun_hm[19200]; Sending message at /usr/local/s1/fib/penl/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 requenceld="1922"][19129] afturneld: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 1:50:20 [inspense 57:HIS[10417] [insta expansed=4"1237"[19127] [IIIV23] (Illumedia tissan, Ale [INFO] AFTER FOUND COMPL. TASK ON SRC: cur_ned=42, cur_mite=42, total_bytes=42, tissan_id_usc=0, tissan_id_etst=-202, teo_id_usc=1, tissan_id_usc=0, tissan_id_us
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 20 21:50:20 filepower SF-IMS[10417]: [meta sequenceld="1920"][19129] situeneld: stream_file [INFO] FILE /var/st/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] intraneld: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 28:15:0.20 [freqperes 5F:M51[0417] [neta requenceds ¹ =1917[1912]] ituaneds itraa_file [INFO] ADDED INIT confirmation to be SRC: cur_read-0, cur_mite=0, total_bytes=0, stream_id_stc=-0, stream_id_stst=202, seq_id_stc=-0, seq_id
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 20 21:50:20 firepower SF-IMS[10417]: [meta requenceId="1917"][19129] situmeeld: stream_file [INF0] Adding SRC Tark 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] siturneld: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 27:59.20 [freqperes 5F:MST[0417] [neta requenceds ¹ =1915 ¹ [19122] itumentid stream_like [INFO] Creating task on SRC for incoming task: cur_read-0, cur_wite-0, total_bytes=0, thream_id_usc=0, stream_id_dest-202, seq_id_dest-0, state-5tate(320) 38 28 1920 101 [Creating task on SRC for incoming task: cur_read-0, cur_wite-0, total_bytes=0, stream_id_usc=0, stream_id_est-202, seq_id_dest-0, state-5tate(320) 38 28 1920 101 [Creating task on SRC for incoming task: cur_read-0, cur_wite-0, total_bytes=0, stream_id_usc=0, stream_id_est-202, seq_id_dest-0, state-5tate(320) 38 28 1920 101 [Creating task on SRC for incoming task: cur_read-0, cur_wite-0, state-10, state-3tate(320) 38 28 1920 [Creating task on SRC for incoming task; cur_read-0, cur_wite-0, state-10, state-3tate(320) 38 28 1920 [Creating task; cur_read-0, cur_wite-0, state-3tate(320) 38 28 [Creating task; cur_read-0, cur_wite-0, state-3tate(320) 38 28 [Creating task; cur_read-0, state-3tate(320) [Creating task; cur_
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] situnneld: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]: [meta sequenceld="11913"][19123] situmekt stream_life [INF0] ELASTIC/FSTREAM request DeNotBlockList validation passed for: /var/si/sidns_download/7cb2ta4a-4c0e-11ee-b245-a2990cdac7a0
09-28-2023	21:50:15	Local7.Debug	172.16.10.2	Sep 28 21:50:20 firepower SF-INS[9765]; [meta sequence[d="1912"]Sethal[10441]; 169593782010.06[1.824, 31]0.94[7814.92]4815.2210.00[0.00]4 .92[1.60]142.39[0]0[0.00]00.00[0]0.020.06[0]255[0.00]0.00[0]60.02[0.06]0]40[16[23.9]0.0[0.00]0]0.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00]0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.06]0]255[0.00[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02[0.00[0]60.02
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]; 1655937820[2]122[1175]0060
09-28-2023	21:50:07	Local7.Debug	172.16.10.2	Sep 28 21:50:12 firepower SF-IMS(9765): [meta sequenceld="1910"]sthd_monitor(9974): sthd 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="1999"]Serbal[10441]; 1695937810[1.02)6.73(32.50]1.921(0021.90)6635.50(0.0000.0011.71]1.60(367.20)15(270)0.000.00000.00)0000.00000.0000.0000.
09-28-2023	21:50:05	Local7.Debug	172.16.10.2	Sep 28 21:50:10 filepower SF-IMS[9765]: [meta sequenceId="1908"]Eventds[10442]: 1695937810[2]12211175[00
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 29 21:50:02 firepower: ActionQueueScrape.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"]sshd_monito(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 sequence!d="1906"]store_allowlist_history finished successfully.
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 20 21:50:01 firepower store_allowlist_history: [meta sequenceId="1905"]Invoking '/usr/local/st/bin/store_allowlist_history: pl'.
09-28-2023	21:49:56	Local7.Debug	172.16.10.2	Sep 28 21:50:01 firepower CR0N0[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 [irepower CR0ND[6893]: [meta sequenceld="1903"](root) CMD [//usr/local/s1/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-IHS[9765]: [neta sequenceld="1902"]Seihal(10441]: 16959370000.5912.46(11.31)0.0677731.6715066.81)0.000.00051.010.00076.411151286(0.000.0000000.03)0.040025500.000.0000000.03)0.040025500.000.0000000.03)0.040025500.000.00000000.03)0.040025500.0000.00000000000000000000000
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]: 1695307800(2122)1175(0)0
09-28-2023	21:49:52	User.Info	172.16.10.2	Sep 28 21:49:57 frepomer: audit_cent.cgi: admin@10.192.201.95, System > Configuration > / Admin/audit_cent.cgi, Page View

syslogサーバで受信できる設定変更の例を次に示します。

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:

トラブルシュート

設定を適用した後、FMCがsyslogサーバと通信できることを確認します。

システムはICMP/ARPおよびTCP SYNパケットを使用して、syslogサーバが到達可能であること を確認します。次に、チャネルを保護している場合、システムはデフォルトでポート514/UDPを 使用して監査ログをストリーミングし、TCPポート1470を使用します。

FMCでパケットキャプチャを設定するには、次のコマンドを適用します。

• tcpdump.このコマンドは、ネットワーク上のトラフィックをキャプチャします

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

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

さらに、ICMP到達可能性をテストするには、次のコマンドを適用します。

ping.このコマンドは、デバイスが到達可能かどうかを確認し、接続の遅延を知るのに役立ちます。

> 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

関連情報

- <u>テクニカル サポートとドキュメント Cisco Systems</u>
- <u>Cisco Secure Firewall Management Centerアドミニストレーションガイド</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。