配置裝置以傳送和檢視FMC上的故障排除系統日 誌

目:	錄	_
<u>簡介</u>	<u>介</u>	
<u>必要</u>	要 <u>條件</u>	
<u>.</u>	<u>需求</u>	
採	<u>採用元件</u>	
<u>功能</u>	能概述	
<u>設定</u>	定 , · · · · · · · · · · · · · · · · · · ·	
驗證	<u>發設定</u>	

簡介

本文檔介紹如何將受管裝置配置為將診斷系統日誌消息傳送到FMC,並在統一事件檢視器中檢視這 些消息。

必要條件

需求

思科建議您瞭解以下主題: ·系統日誌消息 •Firepower Management Center (FMC) •Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本: ·本文檔適用於所有Firepower平台。 ·執行軟體版本7.6.0的安全防火牆威脅防禦虛擬(FTD) ·運行軟體版本7.6.0的安全防火牆管理中心虛擬(FMC) 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。 功能概述

在Secure Firewall 7.6中,將在統一事件檢視器表中新增新的故障排除事件型別。平台設定syslog日 誌記錄配置已擴展,它支援將LINA生成的診斷系統日誌消息傳送到FMC,而不只是傳送VPN日誌。 您可以在運行與FMC 7.6.0相容的軟體版本的任何FTD上配置此功能。由於cdFMC沒有分析工具

,因此不支援cdFMC。

- 由於存在事件卷,「所有日誌」選項限製為緊急、警報和嚴重日誌級別。
- 這些故障排除日誌顯示從裝置傳送到FMC(VPN或其他)的任何系統日誌。
- 故障排除日誌流向FMC,並且在「統一事件檢視」和裝置>故障排除>故障排除日誌下可見。

設定

導覽至FMC Devices > Platform Settings,然後點選策略右上角的Edit圖示。

uludu. Fire cisco _{Devi}	wall Management Center ces / Platform Settings		Q Search Deplo	oy 🔇 🔮 🛞 🕐 🛛 admin ~
^				Object Management
Home				New Policy
Overview	Platform Settings	Device Type	Status	
ad	FTD1_platform_settings	Threat Defense	Targeting 1 device(s)	eted devices 🗗 🖉 🗓
Analysis			op to otto on an ang	
Policies				
Devices				

平台設定策略

移至Syslog > Logging Setup。在Logging to Secure Firewall Management Center下可以看到三個 選項。

Home	FTD1_platform_se	ettings Save	Cancel
	Enter Description	Policy Assign	ments (1)
Overview	APP Inspection	Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers	
III Analysis	Banner	Basic Logging Settings Enable logging	
Policies	DNS External Authentication	Enable logging on the failover standby unit Send syslogs in EMBLEM format	
	Fragment Settings HTTP Access	Send debug messages as syslogs Memory Size of the Internal Buffer (bytes)	
Devices	ICMP Access NetFlow	4096	
Objects	SSH Access	Logging to Secure Firewall Management Center	
1 Integration	SNMP	Off Off VPN Logs	
	SSL Syslog	2 - critical	
	Timeouts	FTP Server Information	
		FTP server buffer wrap	

三個日誌記錄選項

如果選擇All Logs,則可以選擇三個可用日誌記錄級別中的任意一個:緊急事件、警報和嚴重事件 ,並將所有診斷系統日誌消息傳送到FMC(包括VPN)。

								Policy Assign	ments (1)
Overview		Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers	
III Analysis Policies Devices	ARP Inspection Banner DNS External Authentication Fragment Settings HTTP Access ICMP Access NetFlow	Basic Logging Enable logging Enable logging Send syslogs Send debug m Memory Size of th 4096 (4096-52428800)	g Settings g on the failover standby u in EMBLEM format nessages as syslogs se Internal Buffer (bytes)	nit					
Objects	SSH Access SMTP Server	Logging to Se	cure Firewall Mana	gement Cent	er				
5 Integration	SNMP SSL Syslog Timeouts Time Synchronization	Off A A	II Logs VPN Logs	Available	Interface Group	15 C	Sele	cted Interface Groups	

可用的日誌記錄級別

如果選擇VPN Logs,則所有日誌記錄級別均可用,並且可以選擇其中一個。

E2			Policy Assignments (1)
Overview		Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers	
dil .	ARP Inspection	Basic Logging Settings	
Analysis	Banner	Enable logging	
.0.	DNS	Enable logging on the failover standby unit	
Policies	External Authentication	Send syslogs in EMBLEM format	
	Fragment Settings	Send debug messages as syslogs	
=	HTTP Access	Memory Size of the Internal Buffer (bytes)	
Devices	ICMP Access	4096	
	NetFlow	(4098-52428800)	
Objects	SSH Access		
	SMTP Server	Logging to Secure Firewall Management Center	
÷.	SNMP	Off All Logs VPN Logs	
Integration	SSL	Logging Level	
	Syslog	B - errors V	
	Timeouts	0 - emergencies	
	Time Synchronization	1 - alerts	
	Time Zone	2 - critical Available Interface Groups	
	UCAPL/CC Compliance	3 - errors O Search	
	Performance Profile	4 - warnings	
		5 - notifications	
		E. (domation)	
		Add	
		7 - debugging	

可用的日誌記錄級別



附註:當您使用站點到站點或遠端訪問VPN配置裝置時,預設情況下,它會自動啟用向管 理中心傳送VPN系統日誌的功能。您可以將其更改為「所有日誌」,以將除VPN日誌之外 的所有系統日誌傳送到FMC。

可從Devices > Troubleshoot > Troubleshooting Logs訪問這些日誌。

.ılı.ılı. cısco	Firewall Management Center Devices / Troubleshoot / Troubleshooting Logs		Q Search	Deploy 📀 🧬 🐼 🤇	admin ~
Home	e		Bookmark This Pag	e Create Report Dashboard View B 2025-01-15 15:33:00 - 20	ookmarks Search 25-01-16 16:49:00
Overvi	No Search Constraints (Edit Search) iew Table View of Troubleshooting Logs				Static
lil Analys	sis □ ↓ Time ×	Severity $ imes$ Message $ imes$	Ме	essage Class $ imes$ Username $ imes$	Device \times
Policie	₹ 2025-01-15 19:59:43	Alert (Primary) No respo	nse from other firewall (reason code = 4). ha		FTD1
1	₹ 2025-01-15 19:59:27	Alert (Secondary) Disab	ing failover. ha		FTD2
	₹ 2025-01-15 19:59:13	Alert (Primary) No respo	nse from other firewall (reason code = 3). ha		FTD1
Device	₹ 2025-01-15 19:49:12	Alert (Primary) No respo	nse from other firewall (reason code = 3). ha		FTD1
•_=	₹ 2025-01-15 19:43:28	Alert (Secondary) Switc	hing to OK. ha		FTD2
Objec	Image: The second s	Alert (Primary) No respo	nse from other firewall (reason code = 4). ha		FTD1
d -	₹ 2025-01-15 19:42:54	Alert (Secondary) No re	sponse from other firewall (reason code = 4).		FTD2
Integrat	tion ₹ □ 2025-01-15 19:42:25	Alert (Primary) No respo	nse from other firewall (reason code = 4). ha		FTD1
	₹ 2025-01-15 19:41:52	Alert (Secondary) Switc	ning to ACTIVE - HELLO not heard from peer. ha		FTD2
	₹ 2025-01-15 19:41:52	Alert (Secondary) No re:	sponse from other firewall (reason code = 4).		FTD2
	€ 2025-01-15 19:41:51	Alert (Secondary) Switc	ning to OK. ha		FTD2
	₹ 2025-01-15 19:41:50	Alert (Secondary) Switch	ning to OK. ha		FTD2

故障排除日誌的表檢視

Unified Event Viewer頁面上現在有一個新的「故障排除」檢視頁籤。要檢視這些事件,請導航到分析>統一事件>故障排除。

cisco Analys	vall Management Cente is / Unified Events	er		Q Search		Deploy 📀	🐼 🕐 admin ~
Home	Events	g					
	Q Search						☆ 🛞 Refresh
≡≡ Overview	\$14 60 00 00	👬 0) 🗄 14 events				2025-01-16 15:33:4 2025-01-16 16:49:4	4 IST 1h 16m Go Live
dif	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po ICMP Type
Analysis	> 2025-01-16 16:49:27	S Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp
0	> 2025-01-16 16:48:37	S Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp
Policies	> 2025-01-16 16:47:17	S Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp
_	> 2025-01-16 16:46:17	S Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp
Devices	> 2025-01-16 16:43:58	S Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp
2011000	> 2025-01-16 16:43:25	S Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp
•_=	> 2025-01-16 16:40:48	S Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re
Objects	> 2025-01-16 16:39:32	S Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re
	> 2025-01-16 16:37:38	S Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp
Integration	> 2025-01-16 16:36:28	S Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp
	> 2025-01-16 16:35:22	rightarrow Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp
	> 2025-01-16 16:33:10	S Connection	Slock		198.51.100.49	192.0.2.63	3692 / tcp
	> 2025-01-16 16:32:10	S Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re
	> 2025-01-16 16:31:15	\Rightarrow Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp

故障排除檢視

切換到此頁籤後,新的事件型別在表中可見。不能像其他型別那樣在檢視中新增或刪除它,因為它 在故障排除檢視的中心。

.ılı.ılı. cısco	Firewal Analysis /	ll Ma Unifie	inagement Center d Events	ſ		Q Search		Deploy	<u>ଓ</u> ଦ୍ୱି ପୂ	}	admin 🗸
Hom	ie	Eve	nts Troubleshooting								
		Q (Event Type Troubleshoo	ting +						\otimes	Refresh
Overvi	iew	* 399		🗅 – 🛔 🗄 399 events				R	2025-01-15 15:33:44 2025-01-16 16:49:44	IST 1d 1h	Go Live
dil			Time	Event Type	Source IP	Device	Domain	Messag	e	Message	Clas: 🔟
Analy	sis	>	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Primary	/) No response f	ha	1
0		>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Second	lary) Disabling f	ha	
Polici	es	>	2025-01-15 19:59:13	* Troubleshooting		FTD1	Global	(Primary	/) No response f	ha	
		>	2025-01-15 19:49:12	* Troubleshooting		FTD1	Global	(Primary	/) No response f	ha	
Devic	0.0	>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Second	lary) Switching t	ha	
Devic		>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Primary	/) No response f	ha	
•=		>	2025-01-15 19:42:54	* Troubleshooting		FTD2	Global	(Second	iary) No respon	ha	
Objec	sts	>	2025-01-15 19:42:25	* Troubleshooting		FTD1	Global	(Primary	/) No response f	ha	
		>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Second	iary) No respon	ha	
Integra	tion	>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Second	lary) Switching t	ha	
		>	2025-01-15 19:41:51	* Troubleshooting		FTD2	Global	(Second	lary) Switching t	ha	
		>	2025-01-15 19:41:50	* Troubleshooting		FTD2	Global	(Second	lary) Switching t	ha	
		>	2025-01-15 19:41:50	* Troubleshooting		FTD1	Global	(Primary	v) No response f	ha	
		>	2025-01-15 19:41:49	* Troubleshooting		FTD2	Global	(Second	lary) Switching t	ha	
		>	2025-01-15 19:41:48	* Troubleshooting		FTD2	Global	(Second	larv) Switching t	ha	

故障排除事件型別

仍然可以在此「故障排除」檢視中新增和刪除其他事件型別。這樣,您就可以檢視診斷日誌以及其他事件資料。

iliili f	F irewall M a Analysis / Unifi	anagement Cente led Events	r		Q Sea	arch	Deploy 💽 O 🌘	🖗 🕲	admin 🗸
Home	Eve	ents Troubleshooting	-						
Uverview	Q (* 39	× Event Type Troubles	hooting Connection X	Intrusion X +			2025-01-15 2025-01-16	(8) 15:33:44 IST 16:49:44 IST 16 1h	Refresh Go Live
ad		Time	Event Type	Source IP	Device	Domain	Message	Message C	las: 🔟
Analysis	• •	2025-01-16 16:40:48	S Connection	198.51.100.111	FTD1	Global			:
0	>	2025-01-16 16:39:32	S Connection	198.51.100.145	FTD1	Global			1
Policies	>	2025-01-16 16:37:38	S Connection	198.51.100.39	FTD1	Global			+
	>	2025-01-16 16:36:28	S Connection	203.0.113.75	FTD1	Global			1
E Devices	>	2025-01-16 16:35:22	S Connection	203.0.113.153	FTD1	Global			-
	>	2025-01-16 16:33:10	S Connection	198.51.100.49	FTD1	Global			1
* =	>	2025-01-16 16:32:10	S Connection	198.51.100.95	FTD1	Global			-
Objects	>	2025-01-16 16:31:15	S Connection	192.0.2.25	FTD1	Global			
- A.	>	2025-01-15 19:59:43	🛠 Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
Integratio	n >	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Secondary) Disab	bling f ha	
	>	2025-01-15 19:59:13	🛠 Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	>	2025-01-15 19:49:12	* Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Secondary) Switc	hing t ha	
	>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
		101E 01 1E 10-41-EA	SF Traublachapting		ETDO	Clobal	(Canandani) No re	enen he	

其他事件型別

驗證設定

從FMC GUI完成組態後,即可在FTD CLI中,在CLISH或LINA模式下執行show running-config logging和show logging指令以驗證組態。

FTD1# show running-config logging	
logging enable	
logging timestamp	
logging list MANAGER ALL SYSLOG EV	ENT LIST level critical
logging buffered errors	
logging FMC MANAGER ALL SYSLOG EVE	NT LIST
logging device-id hostname	
logging permit-hostdown	
no logging message 106015	
no logging message 313001	
no logging message 313008	
no logging message 106023	
no logging message 710003	
no logging message 302015	
no logging message 302014	
no logging message 302013	
no logging message 302018	
no logging message 302017	
no logging message 302016	
no logging message 302021	
no logging message 302020	

FTD CLI指令

FTD1# show logging							
Syslog logging: enabled							
Facility: 20							
Timestamp logging: enabled							
Timezone: disabled							
Logging Format: disabled							
Hide Username logging: enabled							
Standby logging: disabled							
Debug-trace logging: disabled							
Console logging: disabled							
Monitor logging: disabled							
Buffer logging: level errors, 45 messages logged							
Trap logging: disabled							
Permit-hostdown logging: enabled							
History logging: disabled							
Device ID: hostname "FTD1"							
Mail logging: disabled							
ASDM logging: disabled							
FMC logging: list MANAGER ALL SYSLOG EVENT LIST, 45 messages logged							

FTD CLI指令

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)。