FMC에서 문제 해결 Syslog를 전송하고 볼 디바 이스 구성

목차

<u>소개</u>		
<u>사전 요구 사항</u>		
<u>요구 사항</u>		
<u>사용되는 구성 요소</u>		
<u>기능 개요</u>		
<u>구성</u>		
<u>구성 확인</u>		

소개

이 문서에서는 진단 syslog 메시지를 FMC에 전송하고 Unified Event Viewer에서 볼 수 있도록 관리 되는 디바이스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다. · Syslog 메시지 •FMC(Firepower Management Center) •FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

· 이 문서는 모든 Firepower 플랫폼에 적용됩니다.

· 소프트웨어 버전 7.6.0을 실행하는 FTD(Secure Firewall Threat Defense Virtual)

· 소프트웨어 버전 7.6.0을 실행하는 FMC(Secure Firewall Management Center Virtual) 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 개요

Secure Firewall 7.6의 Unified Event Viewer 테이블에 새로운 Troubleshoot 이벤트 유형이 추가됩니다. 플랫폼 설정 syslog 로깅 컨피그레이션이 확장되었으며 VPN 로그만 전송하는 대신 LINA에서 생성한 진단 syslog 메시지를 FMC로 전송할 수 있습니다. 이 기능은 FMC 7.6.0과 호환되는 소프트웨어 버전을 실행하는 모든 FTD에서 구성할 수 있습니다. cdFMC에는 분석 도구가 없으므로

cdFMC는 지원되지 않습니다.

- All Logs(모든 로그) 옵션은 이벤트 볼륨으로 인한 긴급, 경고 및 위기 로그 레벨로 제한됩니다
- 이 트러블슈팅 로그는 디바이스에서 FMC로 전송된 모든 syslog를 표시합니다(VPN 또는 기 타).
- 문제 해결 로그는 FMC로 이동하며 Unified Event View(통합 이벤트 보기) 및 Devices(디바이 스) > Troubleshoot(문제 해결) > Troubleshooting Logs(문제 해결 로그) 아래에 표시됩니다.

구성

FMC Devices(FMC 디바이스) > Platform Settings(플랫폼 설정)로 이동하고 정책의 오른쪽 상단 모 서리에 있는 Edit(수정) 아이콘을 클릭합니다.

uluulu F	Firewall Devices / F	l Management Center Platform Settings		Q Search	Deploy	⊙∘ (֎	?	admin 🗸
							(Object N	Management
Home									New Policy
Overview	v	Platform Settings	Device Type		Status				
II Analysis		FTD1_platform_settings	Threat Defense		Targeting 1 device(s) Up-to-date on all targeted	devices		₽ ⁄	5
Policies									
Devices									

플랫폼 설정 정책

Syslog > Logging Setup으로 이동합니다. Logging to Secure Firewall Management Center(Secure Firewall Management Center에 로깅)에서 세 가지 옵션을 볼 수 있습니다.

	FTD1_platform_se	ettings	Save Cancel
Home	Enter Description		
			Policy Assignments (1)
Overview		Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings Syslog Set	vers
ahl -	ARP Inspection	Basic Logging Settings	
Analysis	Banner	✓ Enable logging	
Ø	DNS	Enable logging on the failover standby unit	
Policies	External Authentication	Send syslogs in EMBLEM format	
1	Fragment Settings	Send debug messages as syslogs	
Devices	HTTP Access	Memory Size of the Internal Buffer (bytes)	
	ICMP Access	4096	
•_=	NetFlow	(4096-52428800)	
Objects	SSH Access	Logging to Secure Firewall Management Center	
	SMTP Server		
Integration	SNMP	Logging Level	
	Sol	2 - critical V	
	Sysiog		
	mieouts	FTP Server Information	
		FTP server buffer wrap	

All Logs(모든 로그)를 선택하는 경우 사용 가능한 세 가지 로깅 레벨 중 하나를 선택할 수 있습니다. 긴급 상황, 경고, 위험 상황 등 모든 진단 syslog 메시지를 FMC(VPN 포함)로 전송합니다.

								Policy Assignments (1)					
Overview		Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers					
dd	ARP Inspection	Basic Logging	Settings										
Analysis	Banner	Senable logging											
0	DNS	Enable logging on the failover standby unit											
Policies	External Authentication												
1	Fragment Settings	Send debug m	Send debug messages as syslogs										
Devices	HTTP Access	Memory Size of the	e Internal Buffer (bytes)										
2011000	ICMP Access	4096											
•_=	NetFlow	(4096-52428800)											
Objects	SSH Access	Logging to Secure Firewall Management Center											
	SMTP Server	O off O AI	Logs O VPN Logs										
Integration	SNMP	Logging Level											
	Suclea	2 - critical	~										
	Timeouts	0 - emergencies											
	Time Synchronization	1 - slorte											
		2 - critical		Available	Interface Groups	s C'	Selec	cted Interface Groups					

사용 가능한 로깅 레벨

VPN Logs(VPN 로그)를 선택하는 경우 모든 로깅 레벨이 사용 가능하며 그 중 하나를 선택할 수 있 습니다.

			Policy Assignments (1)							
Overview		Longing Setup Longing Destinations Email Setup Event Lists Pate Limit System Settings System Servers								
	ARP Inspection	Desire Langing Destinations Email Detup Event Lists Rate Emit Systog Detungs Systog Detvers								
Analysis	Banner	Basic Logging Settings								
	DNIC	C 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	(4096-52428800)								
Objects	SSH Access									
	SMTP Server	Logging to Secure Firewall Management Center								
÷-	SNMP	Off All Logs OVPN Logs								
Integration	SSL	Logging Level								
	Syslog	3 - errors V								
	Timeouts	0 - emergencies								
	Time Synchronization	1 - alerts								
	Time Zone	2 - critical Available Interface Groups								
	UCAPL/CC Compliance	3 - errors								
	Performance Profile	4 - warnings								
		5 - notifications								
		6 - international								
		7 - debugging								

사용 가능한 로깅 레벨



참고: Site-to-Site 또는 원격 액세스 VPN을 사용하여 디바이스를 구성하면 기본적으로 VPN syslog를 관리 센터에 전송할 수 있습니다. VPN 로그 이외의 모든 syslog를 FMC로 보 내도록 All Logs(모든 로그)로 변경할 수 있습니다.

이러한 로그는 Devices(디바이스) > Troubleshoot(문제 해결) > Troubleshooting Logs(문제 해결 로 그)에서 액세스할 수 있습니다.

.ılı.ılı. cısco	Firewal Devices /	II Mana Troubles	agen :hoot /	nent Center Troubleshooting Logs		Q Search	Deploy	⊙∘ 	@ (admin 🗸
Home	9					Boo	okmark This Page Create Repor 20.	rt Dashboard 25-01-15 15:33	View B :00 - 20	ookmark 25-01-1	s Search 6 16:49:00
Overvi	No B W	Search	Constr /iew o	raints (Edit Search) f Troubleshooting Logs]						51800
lil Analys	is			↓ Time ×	Severity \times	Message ×	Message Class 🛛 🗡	Usernam	e ×	Devic	e ×
Policie	s	÷		2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	. ha			FTD1	
1		÷		2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha			FTD2	
Devie		+		2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha ha			FTD1	
Device	15	÷		2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reason code = 3).	ha			FTD1	
• _		+		2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha			FTD2	
Objec	ts	+		2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha			FTD1	
.		+		2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code =	4). ha			FTD2	
Integrat	ion	÷		2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reason code = 4).	. ha			FTD1	
		+		2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not heard from pe	eer. ha			FTD2	
		+		2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (reason code =	4). ha			FTD2	
		+		2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha			FTD2	
		÷		2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha			FTD2	

문제 해결 로그의 표 보기

이제 Unified Event Viewer 페이지에서 새 문제 해결 보기 탭을 사용할 수 있습니다. 이러한 이벤트 를 보려면 Analysis > Unified Events > Troubleshooting으로 이동합니다.

Gisco Analysis	all Management Cente / Unified Events	r		Q Search		Deploy 💽 🔮	@ @ :	admin 🗸
Home	Events	g						
	Q Search						☆⊗	Refresh
Overview	\$14 60 00	👬 0 👌 14 events				2025-01-16 15:33:4 2025-01-16 16:49:4	4 IST 4 IST 1h 16m	Go Live
ant	Time	Event Type	Action	Reason	Source IP	Destination IP	Source ICMP T	Ро Туре
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	\Leftrightarrow Connection	Block		192.0.2.214	203.0.113.139	8080 /	tcp
Devices	> 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	\Leftrightarrow 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 / 1	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	\Leftrightarrow Connection	Allow		203.0.113.153	192.0.2.132	9876 /	tcp :
	> 2025-01-16 16:33:10	S Connection	Block		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	\Leftrightarrow Connection	Allow		192.0.2.25	203.0.113.249	1234 /	tcp :

문제 해결 보기

이 탭으로 전환하면 테이블에 새 이벤트 유형이 표시됩니다. 다른 유형과 마찬가지로 Troubleshooting 뷰의 중심이므로 뷰에서 추가하거나 제거할 수 없습니다.

.ılı.ılı. cısco	Firewa Analysis /	ll Ma Unifie	nagement Center d Events	·		Q Search		Deploy	ୁତ∘େ 🔮 ଉୂ	0	admin 🗸
Hom	ie	Ever	nts Troubleshooting								
	[Q (Event Type Troubleshoot	ting +						\otimes	Refresh
Overv	iew	* 399	5 6 0 1	🗅 🔺 🗄 399 events				Po Po	2025-01-15 15:33:44 2025-01-16 16:49:44	IST 1d 1h	• Go Live
			Time	Event Type	Source IP	Device	Domain	Messag	ge	Message	Clas:
Analy	sis	,	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Primar	v) No response f	ha	
		>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Secon	darv) Disabling f	ha	
Polici	es	>	2025-01-15 19:59:13	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	-
		>	2025-01-15 19:49:12	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
		>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	
Devic	es	>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
•=		>	2025-01-15 19:42:54	* Troubleshooting		FTD2	Global	(Secon	dary) No respon	ha	1
Objec	ets	>	2025-01-15 19:42:25	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
		>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Secon	dary) No respon	ha	
Integra	tion	>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	
		>	2025-01-15 19:41:51	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	
		>	2025-01-15 19:41:50	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	
		>	2025-01-15 19:41:50	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
		>	2025-01-15 19:41:49	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	
		>	2025-01-15 19:41:48	* Troubleshooting		FTD2	Global	(Secon	dary) Switching t	ha	

문제 해결 이벤트 유형

다른 이벤트 유형은 이 트러블슈팅 보기에서 계속 추가 및 제거할 수 있습니다. 이렇게 하면 진단 로 그를 다른 이벤트 데이터와 함께 볼 수 있습니다.

uludu. Fi	rewall I alysis / Ur	Ma nifie	nagement Center d Events				Q Search	Deploy	<u>o</u> o 🚱	Ø	0	adm	nin ~
Home	Events Troubleshooting												
		Q × Event Type Troubleshooting Connection × Intrusion × +											efresh
Overview	*	399	5 14 6 00	🗅 🐞 🗄 413 event	S				2025-01-15 15: 2025-01-16 16:	33:44 49:44	ST 1d 1	h • G	So Live
ald			Time	Event Type	Source IP	Device	Domain	Ме	ssage		Messa	ge Clas:	ŧ ()]]]
Analysis		>	2025-01-16 16:40:48	S Connection	198.51.100.111	FTD1	Global						1
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						1
		>	2025-01-16 16:36:28	S Connection	203.0.113.75	FTD1	Global						1
Devices		>	2025-01-16 16:35:22	S Connection	203.0.113.153	FTD1	Global						1
		>	2025-01-16 16:33:10	S Connection	198.51.100.49	FTD1	Global						+
• =		>	2025-01-16 16:32:10	S Connection	198.51.100.95	FTD1	Global						1
Objects		>	2025-01-16 16:31:15	S Connection	192.0.2.25	FTD1	Global						1
A.		>	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Pri	mary) No respons	e f	ha		
Integration		>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Se	condary) Disablin	g f	ha		
		>	2025-01-15 19:59:13	* Troubleshooting		FTD1	Global	(Pri	mary) No respons	e f	ha		
		>	2025-01-15 19:49:12	* Troubleshooting		FTD1	Global	(Pri	mary) No respons	e f	ha		
		>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Se	condary) Switchir	ıg t	ha		
		>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Pri	mary) No respons	e f	ha		
		•	101E 01 1E 10-41-E4	** Tranklashasting		CTD0	Clobal	10-	andara) No roon	~~	ha		

기타 이벤트 유형

구성 확인

FMC GUI에서 컨피그레이션을 완료하면 FTD CLI에서 show running-config logging 및 show logging 명령을 CLISH 또는 LINA 모드로 실행하여 확인할 수 있습니다.

FTD	1# show	running-	-config logging
log	ging ena	able	
loq	ging tir	nestamp	
log	ging lis	st MANAGE	ER_ALL_SYSLOG_EVENT_LIST level critical
loq	ging but	ffered er	rrors
log	ging FM(C MANAGEF	R ALL SYSLOG EVENT LIST
log	ging dev	vice-id h	nostname
log	ging per	rmit-host	tdown
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 명령

FTD1# show logging								
yslog 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 명령

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.