Configurar dispositivos para enviar e visualizar syslogs de solução de problemas no FMC

Contents	
Introdução	
Pré-requisitos	
Requisitos	
Componentes Utilizados	
<u>Visão geral do recurso</u>	
Configurar	
Verificar a configuração	

Introdução

Este documento descreve como configurar dispositivos gerenciados para enviar mensagens de syslog de diagnóstico ao FMC e visualizá-las no Visualizador de Eventos Unificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:
Mensagens de syslog
Firepower Management Center (FMC)
Firepower Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- \cdot Este documento se aplica a todas as plataformas Firepower.
- · Secure Firewall Threat Defense Virtual (FTD), que executa a versão 7.6.0 do software

· Secure Firewall Management Center Virtual (FMC), que executa a versão 7.6.0 do software As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do recurso

No Secure Firewall 7.6, um novo tipo de evento Solução de problemas é adicionado à tabela Unified Event Viewer. A configuração de registro de syslog de configurações de plataforma foi estendida e suporta o envio de mensagens de syslog de diagnóstico geradas por LINA para o FMC, em vez de apenas registros VPN. Este recurso pode ser configurado em qualquer FTD que execute uma versão de software compatível com o FMC 7.6.0. O cdFMC não é suportado porque o cdFMC não tem ferramentas de análise.

- A opção Todos os registros está limitada aos níveis de registro de emergência, alerta e crítico devido ao volume de eventos.
- Esses registros de solução de problemas mostram qualquer syslog enviado do dispositivo para o FMC (VPN ou outro).
- Os registros de solução de problemas fluem para o FMC e são visíveis no Unified Event View e em Devices > Troubleshoot > Troubleshooting Logs.

Configurar

Navegue até FMC Devices > Platform Settings e clique no ícone Edit no canto superior direito da política.

cisco Devices /	ll Management Center Platform Settings		Q Search Deploy 🕚 🖗 🕅						
Home					Object Management				
					New Policy				
Overview	Platform Settings	Device Type	Status						
III Analysis	FTD1_platform_settings	Threat Defense	Targeting 1 de Up-to-date of	evice(s) n all targeted devices	₽ ₽				
Policies									
Devices									

Política de Configurações de Plataforma

Vá para Syslog > Logging Setup. Você pode ver três opções em Logging to Secure Firewall Management Center.

	FTD1_platform_set	tings	Save Cancel
Home	Enter Description		
			Policy Assignments (1)
Overview		Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings	Syslog Servers
ald	ARP Inspection	Basic Logging Settings	
Analysis	Banner	C Enable logging	
0	External Authentication	Enable logging on the failover standby unit	
Policies	Fragment Settings	Send syslogs in EMBLEM format	
-	HTTP Access	Memory Size of the Internal Buffer (bytes)	
Devices	ICMP Access	4096	
• 	NetFlow	(4096-52428800)	
Objects	SSH Access	Logging to Secure Firewall Management Center	
5	SNMP	Off All Logs VPN Logs	
Integration	SSL	Logging Level	
	Syslog	2 - critical V	
	Timeouts	FTP Server Information	
		FTP server buffer wrap	

Se você selecionar All Logs, poderá selecionar qualquer um dos três níveis de log disponíveis: emergências, alertas e mensagens críticas e enviar todas as mensagens de syslog de diagnóstico para o FMC (incluindo VPN).

								Policy Assignments (1)
Overview		Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers
III Analysis	ARP Inspection Banner	Basic Logging	g Settings					
Policies	DNS External Authentication	Enable logging	a g on the failover standby ur in EMBLEM format	nit				
Devices	Fragment Settings HTTP Access ICMP Access	Send debug n Memory Size of th	nessages as syslogs ne Internal Buffer (bytes)					
©_≡ Objects	NetFlow SSH Access SMTP Server	(4096-52428800)	ocure Firewall Manag	gement Cent	er			
5. Integration	SNMP SSL Syslog	Off Off A Logging Level	II Logs O VPN Logs					
	Timeouts Time Synchronization	0 - emergencies 1 - alerts 2 - critical		Available	Interface Group	95 C	Sele	cted Interface Groups

Níveis de log disponíveis

Se você selecionar VPN Logs, todos os níveis de registro estarão disponíveis e um deles poderá ser selecionado.

E1			Policy Assignments (1)
Overview		Longing Setup Longing Destinations Email Setup Event Lists Pate Limit System Settings System Services	
did.	ARP Inspection	Basic Logging Settings	
Analysis	Banner	S 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 Auglitable Interface Country C Selected Interface Country	
	UCAPL/CC Compliance	3 - errors Q Search	
	Performance Profile	4 - warnings	
		5 - notifications	
		6 - informational	
		7 - debugging Add	
		·	

Níveis de log disponíveis



Note: Quando você configura um dispositivo com VPN de acesso remoto ou de site a site, ele permite automaticamente o envio de syslogs de VPN para o centro de gerenciamento por padrão. Você pode alterá-lo para All Logs (Todos os registros) para enviar todos os syslogs além dos registros VPN ao FMC.

Esses registros podem ser acessados em Devices > Troubleshoot > Troubleshooting Logs.

ဂျာဂျာဂ င၊sco	Firewall Devices / Tr	Mana	agen hoot /	nent Center Troubleshooting Logs		Q Sear	ch	Deploy	ം 🖗 ത്	0	admin ~
Home	e						Bookmark This Pa	ge Create Report I 2025-	Dashboard Vie 01-15 15:33:00	w Bool - 2025	kmarks Search -01-16 16:49:00 Static
Overvi	No S	Search (Table V	Consti 'iew o	raints (Edit Search) f Troubleshooting Logs]						orano
lil Analys	sis			\downarrow Time \times	Severity \times	Message ×	м	lessage Class $ imes$	Username	×	Device $ imes$
Policie	es	÷		2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reaso	n code = 4). ha	a			FTD1
(÷		2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha	Э			FTD2
Dovice		÷		2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reaso	n code = 3). ha	a			FTD1
Device	25	÷		2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reaso	n code = 3). ha	9			FTD1
		÷		2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha	а			FTD2
Objec	ts	÷		2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reaso	n code = 4). ha	а			FTD1
5 -		÷		2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (rea	ason code = 4). ha	а			FTD2
Integrat	tion	÷		2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reaso	n code = 4). ha	а			FTD1
		÷		2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not he	eard from peer. ha	a			FTD2
		÷		2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (rea	ason code = 4). ha	a			FTD2
		÷		2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha	a			FTD2
		÷		2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha	а			FTD2

Visão em Tabela dos Logs de Troubleshooting

Uma nova guia de exibição Solução de problemas agora está disponível na página Unified Event Viewer. Para exibir esses eventos, navegue até Análise > Eventos unificados > Solução de problemas.

cisco Analys	vall Management Cente is / Unified Events	r		Q Search		Deploy 🕐 🧐	፟፼ () admin ∽
Home	Events	g					
Overview	Q Search	₩0 🗄 14 events				2025-01-16 15:33:44 2025-01-16 16:49:44	☆ ⊗ Refresh IST IST 1h 16m ● Go Live
dil	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	\Leftrightarrow 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
501003	> 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 / tcp
Integration	> 2025-01-16 16:36:28	S Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp
5	> 2025-01-16 16:35:22	S 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	S Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp

Exibição de Solução de Problemas

Um novo tipo de evento estará visível na tabela quando você alternar para esta guia. Ele não pode ser adicionado ou removido da exibição como os outros tipos, pois é central para a exibição Solução de problemas.

.ı ı.ı ı. cısco	Firewa Analysis /	ll Ma Unifie	nagement Center	ſ		Q Search		Deploy	⊙∘ ₽ <	୭ ଡ∣	admin 🗸
Hom	e	Eve	nts Troubleshooting								
		Q (Event Type Troubleshoo	ting +						8	Refresh
Overvi	iew	* 399	5 6 0	🗅 🔹 🗄 399 events				6	2025-01-15 15:33:4 2025-01-16 16:49:4	44 IST 1d 1h	Go Live
dil			Time	Event Type	Source IP	Device	Domain	Messag	je	Message	Clas: 🔳
Analys	sis	>	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	1
0		>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Second	dary) Disabling f.	ha	
Policie	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	
Device	0.0	>	2025-01-15 19:43:28	* Troubleshooting		FTD2	Global	(Second	dary) Switching t	ha	
Device	63	>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
•=		>	2025-01-15 19:42:54	* Troubleshooting		FTD2	Global	(Second	dary) No respon.	ha	
Objec	ts	>	2025-01-15 19:42:25	* Troubleshooting		FTD1	Global	(Primar	y) No response f	ha	
		>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Second	dary) No respon.	ha	
Integrat	tion	>	2025-01-15 19:41:52	* Troubleshooting		FTD2	Global	(Second	dary) Switching t	ha	
		>	2025-01-15 19:41:51	* Troubleshooting		FTD2	Global	(Second	dary) Switching t	ha	
		>	2025-01-15 19:41:50	* Troubleshooting		FTD2	Global	(Second	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	(Second	dary) Switching t	ha	
		>	2025-01-15 19:41:48	* Troubleshooting		FTD2	Global	(Second	tarv) Switching t	ha	

Troubleshooting de Tipo de Evento

Outros tipos de evento ainda podem ser adicionados e removidos desta exibição de Solução de problemas. Isso permite que você visualize logs de diagnóstico juntamente com outros dados de evento.

cisco Analy	wall Ma sis / Unifi	anagement Cente Ied Events	r		Q Sea	rch	Deploy 🔿 🍳	🖗 🕲	admin 🗸
Home	Eve	ents Troubleshooting	9						
	Q	× Event Type Troubles	hooting Connection X	Intrusion \times +				8	Refresh
Overview	* 39	19 5, 14 🔞 🔍 0	🗅 🗯 🗄 413 event	S			2025-01-15 2025-01-16	15:33:44 IST 1d 1h 16:49:44 IST 1d 1h	• Go Live
dif		Time	Event Type	Source IP	Device	Domain	Message	Message	Clas: 📶
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			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			1
* =	>	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			-
A.	>	2025-01-15 19:59:43	* Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
Integration	>	2025-01-15 19:59:27	* Troubleshooting		FTD2	Global	(Secondary) Disat	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) Swite	hing t ha	
	>	2025-01-15 19:42:58	* Troubleshooting		FTD1	Global	(Primary) No respo	onse f ha	
	•	2026 01 16 10-42-64	Sk Troubloobooting		CTD0	Clobal	(Canandani) No re	enen he	

Outros tipos de evento

Verificar a configuração

Depois que a configuração é feita na GUI do FMC, ela pode ser verificada na CLI do FTD

executando os comandos show running-config logging e show logging no modo CLISH ou LINA.

FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
LOGGING FMC MANAGER_ALL_SYSLOG_EVENT_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

Comando CLI de FTD

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.