Converter em contêiner (modo MI) no FTD 7.6 com GUI

Contents

Introdução Pré-requisitos, plataformas suportadas, licenciamento Plataformas mínimas de software e hardware **Licenciamento Componentes Utilizados** Informações de Apoio O que há de novo? Plataformas com suporte a várias instâncias de FTD Diferenças entre as séries 3100 e 4200 Implantações suportadas Descrição do recurso e passo a passo Especificações da instância do 4200 Series Máx. de suporte a instâncias Tamanhos de Instância de FTD Alocações de Núcleo Snort de Lina (Plano de Dados) Configurar Visão geral da configuração Converta o 4200 Series para o modo de várias instâncias no FMC Converter um único dispositivo Converter mais de um dispositivo (conversão em massa) Monitorando o Andamento e Finalizando Página de visão geral do chassi do FMC Visão geral da página de visão geral do chassi do FMC Seções da guia Resumo da página Chassis Gerenciar interfaces Resumo da guia Interfaces Modificar configurações de interface física Gerenciar Subinterface Gerenciar EtherChannel Configurações do Dispositivo de Sincronização Suporte A Hot Swap/Break-Out Netmod 4200 nativo suporta EPM Hot Swap e Breakout OIR: Habilitar/Desabilitar Confirmação do EPM Ativação Completa do EPM: Notificação de Interface Recebida Notificação de Alteração da Interface do EPM

Página Opções de quebra/junção no chassi

Alterações de interface após quebra/junção

Impacto de alterações de interface na instância

Gerenciamento de instâncias

Criar uma instância

Editar uma instância

Excluir instância

Configuração de SNMP

Importação/exportação de chassi

Exportar configuração

Importar configuração

O que você precisa saber sobre importação/exportação de chassis

Política de configurações da plataforma do chassi

Configurações da plataforma do chassi: DNS

Configurações da plataforma do chassi: SSH

Configurações da plataforma do chassi: lista de acesso SSH

Configurações da plataforma do chassi: sincronização de horário

Do NTP do Management Center

No servidor NTP personalizado

Configurações da plataforma do chassi: fusos horários

Configurações da plataforma do chassi: Syslog

Configurações da plataforma do chassi: salvar e implantar

Cancelando o registro do chassi

Converter de Várias Instâncias para o Modo Nativo

APIs FMC Rest

APIs REST para conversão de nativo em várias instâncias

APIs REST para gerenciamento de chassi

APIs REST para gerenciamento de Netmods (módulos de rede)

APIs REST para gerenciamento de instâncias

APIs REST para gerenciamento SNMP

Resumo de APIs REST para busca

APIs REST para gerenciamento de interface

Atualizar interface física

Configurar subinterfaces

Configurar Interfaces EtherChannel

Interfaces de interrupção/junção de APIs REST Fluxo REST para quebra de interface

Fluxo REST para junção de interface

Sincronizar APIs REST de Dispositivo

Solução de problemas/diagnósticos

Log FXOS

Registro do CVP

Solução de problemas do chassi

Exemplos de Problemas com Troubleshooting de Passo a Passo

Registro automático de falha de chassi no FMC

Solução de problemas

Autorregistro de instância no CVP

Solução de problemas

Registro de dispositivo nativo no FMC

Solução de problemas	
Referências úteis	
Opções de interface e alta disponibilidade	
Opções de interface	
Independente ou alta disponibilidade	
Aproveitando as interfaces de gerenciamento duplas	
Informações de rastreamento interno	

Introdução

Este documento descreve como configurar um contêiner (modo de várias instâncias) no Firepower 4200 série de firewall com FTD 7.6 e detalhes relacionados.

Pré-requisitos, plataformas suportadas, licenciamento

Plataformas mínimas de software e hardware

Manager(s) and Version (s)	Application (ASA/FTD) and Minimum Version of Application	Supported Platforms
• FMC 7.6.0	• FTD 7.6.0	4200 Series 4215, 4225, 4245



Observação: Não há suporte para Várias Instâncias com o FDM em nenhuma plataforma.

Licenciamento

- As licenças de recursos são atribuídas manualmente a cada instância, mas você consome apenas uma licença por recurso por dispositivo 4200-series.
 - Por exemplo, para uma série 4200 com 3 instâncias de FTD, você só precisa de uma licença de URL, independentemente do número de instâncias em uso, desde que esteja no mesmo FMC.
- Todas as licenças são consumidas por dispositivo 4200 Series e não por instância de contêiner, desde que estejam no mesmo FMC. Portanto, para todas as instâncias em dispositivos 4200 Series, é recomendável usar o mesmo FMC devido à implementação da licença.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

- O FTD já suporta a Multi-Instância (MI) em modelos 3100 (assim como as séries 9300 e 4100), mas não há suporte para a série 4200.
- Os modelos 4200 são suportados apenas no modo nativo no FMC.
- Não há provisão para criar várias instâncias no 7.4.x no 4200.
- Várias Instâncias (MI) no 3100 eram suportadas a partir da versão 7.4.1.
 - As instâncias podem ser criadas e gerenciadas usando o FMC (ao contrário das séries 9300 e 4100, em que o FCM deve ser usado).
 - O FXOS pode ser atualizado, quando no modo MI, através da GUI do chassi de atualização do FMC.
 - A conversão para o modo MI é feita por meio de uma CLI.

O que há de novo?

- Você pode provisionar e gerenciar instâncias de MI na série 4200.
- FMC Solução única de gerenciamento para a série 4200 (modo MI) e instâncias de FTD
- Permitir a conversão em massa e única de dispositivos nativos para o modo MI no FMC para dispositivos das séries 3100 e 4200
- Mercado-alvo: grandes/grandes empresas borda da Internet, data center

Plataformas com suporte a várias instâncias de FTD

Platform	FTD Version	FTD Multi-Instance Support	Management Solution
Virtual	-	No	-
FPR1000	-	No	-
FPR2100	(not supported in 7.6)	No	-
3105		No	
3110, 3120, 3130, 3140	FTD 7.4.1	Yes	FMC
FPR4100	FTD 6.3.0	Yes	FCM & FMC
4215, 4225, 4245	FTD 7.6.0	Yes	FMC
FPR9300	FTD 6.3.0	Yes	FCM & FMC

Diferenças entre as séries 3100 e 4200

- O 4200 tem duas interfaces de gerenciamento, permitindo o uso de uma para gerenciamento e outra para eventos.
 - As interfaces Management1/1 e Management1/2 são inicializadas para todas as instâncias de contêiner de FTD.
 - Uma ou ambas as interfaces de gerenciamento podem ser usadas no modo MI.
 - Gerenciamento1/1 para Gerenciamento e Eventos ou
 - Gerenciamento1/1 pode ser usado para gerenciamento e Gerenciamento1/2 para eventos, nesse caso.
 - As rotas estáticas precisam ser definidas para rotear o tráfego usando a interface 1/2 de gerenciamento.
- Devido ao tamanho maior, mais instâncias podem ser criadas no 4200 do que no 3100

Implantações suportadas

- Gerencie a Série 4200 (modo MI) com Instância(s) Autônoma(s) de FTD
- Gerenciar 4200 Series (modo MI) com Instância(s) HA FTD*



Nota: Como é o caso da série FPR4100, no caso do FTD-HA, os nós primário e

secundário devem estar em dois dispositivos 4200 Series (modo MI) diferentes. Além disso, o agrupamento MI não é suportado nesta versão.

Descrição do recurso e passo a passo

Alterações na configuração de várias instâncias na versão 7.6.0:

- Suporte para 4200 Series no modo MI
- Alterações do CVP relativas à gestão em modo IA da série 3100:
 - Conversão do dispositivo do modo Nativo para o modo MI no FMC
 - Readiness Verifica se o dispositivo pode ser convertido para o modo MI
 - Autorregistrar instância de FTD no FMC após a conversão

Especificações da instância do 4200 Series

Máx. de suporte a instâncias

Platform	Maximum Instance Count	Maximum Logical CPU Cores Supported
FP4215	10	62
FP4225	15	126
FP4245	34	254

A densidade da instância é determinada por dois fatores principais:

1. A quantidade de núcleos de CPU e a quantidade de espaço em disco em uma determinada plataforma

2. Quantos desses recursos estão disponíveis para provisionamento em instâncias. O menor tamanho de instância requer 3 núcleos de CPU física (6 lógicos) e 48 GB de espaço em disco.

Tamanhos de Instância de FTD

Platform	4215	4225	4245
Total CPU cores	32	64	128
Available CPU cores for FTD	30	62	126
Total RAM (GiB)	222	445	875
FXOS RAM (GiB)	6	6	6
DMA RAM (GiB)	11	39	78
Available RAM for FTD (GiB)	7	7	7
Available Disk space for FTD (GiB)	660	864	1794
Max Instances	10	15	34

Alocações de Núcleo Snort de Lina (Plano de Dados)

	4215	4225	4245			
Tamanho da Instância	Núcleos do plano de dados	Núcleos de Snort	Núcleos do plano de dados	Núcleos de Snort	Núcleos do plano de dados	Núcleos de Snort
6	2	2	2	2	2	2
8	2	4	2	4	2	4
10	4	4	4	4	4	4
12	4	6	4	6	4	6
14	6	8	6	6	6	6
16	6	8	6	6	8	8
18	8	10	8	8	8	10

20	8	10	8	8	10	10
22	10	12	10	10	10	12
24	12	12	10	10	10	12
26	12	14	12	12	12	12
28	14	14	12	14	12	14
30	14	16	14	14	14	14
32	14	16	14	16	14	16
34	16	16	16	16	16	16
36	16	18	16	18	16	18
38	18	18	18	18	18	18
40	18	20	18	20	18	20
42	20	20	20	20	20	20
44	20	22	20	22	20	22
46	22	22	22	22	22	22
48	22	24	22	24	22	24
50	24	24	24	24	24	24
52	24	26	24	26	24	26
54	26	26	26	26	24	26

56	26	28	26	28	26	28
58	28	28	28	28	28	28
60	28	30	28	39	28	30
62	30	30	30	30	30	30
64			30	32	30	32
66			30	34	30	34
68			32	34	32	34
70			32	36	32	36
72			34	36	34	36
74			34	38	34	38
76			36	38	36	38
78			36	40	36	40
80			38	40	38	40
82			38	42	38	42
84			40	42	40	42
86			40	44	40	44
88			42	44	42	44
90			42	46	42	46

92		44	46	44	46
94		44	48	44	48
96		46	48	46	48
98		46	50	46	50
100		48	50	48	50
102		48	52	48	52
104		50	52	50	52
106		50	54	50	54
108		52	54	52	54
110		52	56	52	56
112		54	56	54	56
114		54	58	54	58
116		56	58	56	58
118		56	60	56	60
120		58	60	58	60
122		58	62	58	62
124		60	62	60	62
128				60	64

130			60	66
132			62	66
134			62	68
136			64	68
138			64	70
140			66	70
142			66	72
144			68	72
146			68	74
148			70	74
150			70	76
152			72	76
154			72	78
156			74	78
158			74	80
254			120	130

Configurar

Visão geral da configuração

- 1. Registrar dispositivo 4200 Series (modo nativo) no FMC
- 2. Novo! No FMC, selecione e converta o dispositivo do modo Nativo para o modo MI
- 3. Novo! Registros automáticos do chassis do IA para o CVP após conversão
- 4. Atualizar interface(s) física(is)
- 5. Criar instância(s) de FTD e atribuir interface(s)
- 6. Criar/Atualizar/Excluir canal de porta e subinterfaces do FMC
- 7. Definir configurações da plataforma
- 8. Implantar alterações de configuração no dispositivo
- 9. Instância(s) do FTD registra(m) automaticamente no FMC

Converta o 4200 Series para o modo de várias instâncias no FMC

Por padrão, os 4200s estão no modo nativo.

- 1. Conecte-se ao dispositivo e crie um gerenciador (já documentado).
- 2. Registrar o dispositivo nativo no CVP (já documentado).
- 3. Converter em Várias Instâncias usando FMC.
- 4. No FMC, selecione o(s) dispositivo(s) que precisa(m) ser convertido(s) em Várias instâncias e acione a conversão. É possível selecionar um ou mais de um dispositivo.



Observação: alternar entre o modo nativo para o modo MI redefine TODA a configuração no chassi. A conversão do modo MI para o modo nativo ainda é feita via CLI.

Converter um único dispositivo

1. Para iniciar a conversão, navegue até Devices > Device management.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
4215_Native_Chassis Short 3 192.168.1.80 - Routed	Firewall 4215 Threat Defense	7.6.0	Manage	Essentials, Malware (1 more)	None	e© Delete	1
On successful regis Series (Native mod listed in the device Right click the drop select the Convert	stration, 4200 e) device will be listing page. down menu and to Multi-Instance			Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor		Packet Tr Poket Cr Revert Up Heath Mr Troublesh	icer phure grade rittor Multi-instance oct Files

2. Valide o dispositivo selecionado e clique em Continuar:



validar dispositivos selecionados

3. Verificação de preparação e conversão inicial:

Step 1: Set the name of the MI Chassis after conversion.	5 Threat De Convert to Multi-Instance Mode Selected device name 4215_Native_Chassis Configured device name *	Essentials, M Current selected device
	Cancel Convert to Multi-int	Step 2: Hover over the icon next to the name to check whether the device is ready for conversion.
Step 3: Clic Instance to device.	k on Convert to Multi- start conversion for the	

verificação de prontidão

Converter mais de um dispositivo (conversão em massa)

1. Selecionar dispositivos:

View By: Group								Migrate Deploy	ment History
All (2) • Error (2) • V	/arning (0) © Offline (0) ® Normal	(0) • Deployment Pending (0) •	Upgrade (0)	 Snort 3 (2) 				Q. Search Device	Add 👻
Collaose All 2 Devices Selected	Select Bulk Action							Download De	vice List Report
Name Upgrade to Upgrade To	Snort 3 treat Defense Software	Model	Version	Chassis	Licenses		Access Control Policy	Auto RollBack	
Upgrade F	KOS and Firmware (Chassis Only)								
Edi Deproy 4215_Native_Chas 192.168.1.80 - Rou	is Short 3	Firewall 4215 Threat Defense	7.6.0	Manage	Essentials, Malwa	are (1 more)	register_192.168.1.80_1701072	Q+	11
Native_Chapels_2 192.168.1.106 - Ho	Snort 3	Firewall 3130 Threat Defense	7.6.0	Manage	Essentials, Malwa	are (1 more_)	register_192.168.1.106_170107	4Q	11
					Ste	ep 3: Af	ter successful	l registra	tion
Step 1: Successfully register multiple Native mode devices	Step 2: S convert fr next to th	elect the device om native to MI em.	s you using	want to the check box	of se co	multiple lecting r nversior	e native device multiple chass n, click on the	es and is for drop-do	wn
on FMC.	Here, bot	h Ungrouped 42	00s a	re picked.	the	enu to s e "Conv tion	elect bulk acti ert to Multi-In:	on and s stance"	elect

2. Confirmar seleção:



3. Verificação de preparação e início da conversão:



Monitorando o Andamento e Finalizando

1. Notificação de início de conversão:

Firewall Management Center Overview Analysis	Policies Devices Objects	Integration	Deploy Q 🧳 🏟 admin - 🖞 thete SECURE
View By: Group			Deployments Upgrades Health Tasks Show Pop-up Notifications Deployments Upgrades Deployments Deployments
All (1) • Error (1) • Warning (0) Offline (0) • Normal (0) Collaose All	 Deployment Pending (0) Upgrade (0)) • Snort 3 (1)	Switch Mode Conversion of 192,168,1.80 in progress Status: Fetching configuration data from the device
Name Vigrouped (1)	Model Version	n Chassis	Switch Mode Chassis Conversion Chassis Conversion tarted for 1 device(s) 10s
192.168.1.80 Snort 3 192.168.1.80 - Routed	Firewall 4215 Threat Defense 7.6.0	N/A	No more older tasks
		/	
			Remove completed tasks
Once the conversion is trigg	gered, the		
status can be monitored us Task Manager.	ing the		

2. Autorregistro do chassis:

Firewall Management Center Overview Analysis	Policies Devices O	bjects Inte	egration	Deploy Q 🔮 🌣 🚳 admin ~ 讨 🔅 SECURE
View By: Group				Deployments Upgrades I Health Tasks ± C Show Pop-up Notifications
All (1) • Error (0) • Warning (0) • Offline (0) • Normal (1)	 Deployment Pending (0) 	rade (0)		Stotal 0 waiting 2 running 0 retrying 3 success 0 failures Q, Filter
Collacse All				Discovery 192.168.1.80 - Discovery from the device is successful. 15s ×
Kame Vugrouped (1)	Model	Version	Chassis	Register Registration 192.164.1.80: Successfully registered
192.168.1.80 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	Switch Mode Conversion of 192.168.1.80 in progress Status: Trying chassis registration for 192.168.1.80. try 1 of 3 times
Device gets unregistered as device and automatically ge	s a single			Register Unregistration Unregistration Unregistration completed. 192.168.1.09 - Did not update device
registered as a Chassis.				Remove completed tasks
Now the Model column inclute the model and "Multi-Instant Supervisor".	udes both ice			

3. Notificação pós-conversão:

Firewall Management Center Overview Analysis	Policies Devices Ob	jects Inte	gration	Deploy Q 🔗 🌣 🕢 admin 🗸 👘 SECU	IRE
View By: Group •	andrement Practice (0)	ada (0)		Deployments Upgrades Health Tasks ±	•
Collacse All	opoyment Penting (o)	ue (0)		Switch Mode Chassis Conversion Summary Success:1 Falled: 0	×
Vame	Model	Version	Chassis	Switch Mode Conversion of 192.168.1.80 is successful 14m 31s It is added with name 192.168.1.80	×
• 192.168.1.80 • 192.168.1.80 • Successful Conversion Notific	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	Discovery 192.168.1.80 - Discovery from the device is successful. 15s	×
with number of devices conve successfully.	erted			Register Registration 192.164.140: Successfully registered 193	×
				Remove completed tasks	

Página de gerenciamento de dispositivos resultante listando os dispositivos da série 4200 (modo MI):

Ę	Firewall Management Center Overview Analysis	Policies Devices Obj	ects Integ	ration		Deploy Q 💞 🌣	admin v deab	SECURE
Vie	w By: Group +						Migrate Deployme	nt History
	All (1) • Error (0) • Warning (0) = Offline (0) • Normal (1) • De	ployment Pending (0) • Upgra	de (0)			Q	Search Device	Add 🔻
Gel	acte All						Download Device	List Report
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (1)							
	192.168.1.80 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	1

Página de visão geral do chassi do FMC

Visão geral da página de visão geral do chassi do FMC

A página de visão geral do chassi do FMC apresenta um resumo completo do dispositivo 4200 Series (modo MI). Ele inclui:

- Visão pictórica do painel traseiro do dispositivo, incluindo módulos de rede disponíveis
- Resumo de falhas, com sua criticidade
- · Resumo da interface, status
- resumo da instância de FTD, status
- Estatísticas de hardware incluindo VENTILADOR, fonte de alimentação, memória, uso da CPU e armazenamento

Clique em Gerenciar para navegar até Visão geral do chassi:

View	By: Group 🔻							,
A	ll (1) • Error (0) • Warning (0) • Offline (0)	Normal (1) Deploy	ment Pendir	ng (0) • Upgrade (0)		G	Search Device	Add 🔻
Collar	ise All						Download Devi	ice List Report
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	\vee Ungrouped (1)							
	4215_WA_Chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	1
	From the Dev 4200 Series	vice Mana (MI mode)	gem) Cha	ent page, cl assis (device	ick 'Manag e) overviev	ge' to view v.	'	

Guia de resumo da página do chassi:

Chassis	Manager: 192.16	8.1.80 © Connected			Top section displ number Tabs to focus on spe	ays chassis name and model
Cisco Secure Fire Summary	mail (215 Threat Defense Mult) Interfaces Instances	System Configuration	0 verse: 7.4.8 (ball 1406)		management: Summ and System Configu Pictorial represent network module, a user will see CPU	ary, Interfaces, Instances, ration. ation of chassis back plane, nd interface status. Also, core utilisation details
	Faults 1 /1 Unacknowledged	Categories 1 State 2004 Categories Parks Categories (State 2004) Categories (State 2004) Cat	e 0 t2 Gran Laws Take addres Upp: 3 1 Indicate 2 Upp: 3 1 Indicate 2 Upp: 1 1 Indicate 2 Upp: 1 1 Indicate 2 Upp: 1 1 Indicate 2 Upp: 1 2	Power Models2 Text Text Distances Dist Distances Distances Distances Distances	Live mass or 13 Mar 2003 12 Ja stances found 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tile layout provides more granular details on Faults, Interfaces and Instances. Bottom red line on each tile indicates more focus required on respective section
	Hardware Statistics - C ² Security Eng	1 of 1 operable e @ Excellent	Power Supplies		12 of 12 operable Excellent	One place for all hardware statistics.

Seções da guia Resumo da página Chassis

A guia Resumo contém seções. Clique para obter mais detalhes:

- Painel traseiro
- Falhas
- Interfaces
- Instâncias
- Estatísticas de hardware

As seções são mapeadas por número conforme mostrado nesta imagem:



1. Vista de retaguarda:



2. Seção das falhas:



3. Seção Interfaces:





A transição de instâncias de off-line para on-line é mostrada na imagem anterior.

- Depois de provisionado (1)
- A instância fica offline até ficar Online (2)
- Os estados intermédios também são refletidos (3)
- 5. Estatísticas de hardware:

								Networ 1/1	rk Module 1	4		
	La Las lans			Detailed H	ardware Stat	stics						
A 141 amerika				Security Er	ngine F	ans Power	Supplies	CPU	Memory S	orage		
				Name	Fan	Operabil	Operatio	Power	Thermal	Model	Vendor	
				Fan Tray	Fan-1	operable	operable	on	ok	N/A	N/A	
				Fan Tray	Fan-2	operable	operable	on	ok	N/A	N/A	
	Faults		Live status at: 21	Fan Tray	Fan-3	operable	operable	on	ok	N/A	N/A	
		Categorized Faul	ts	Fan Tray	Fan-4	operable	operable	on	ok	N/A	N/A	
		e an emu	A 0/0 - MA	Fan Tray	Fan-1	operable	operable	on	ok	N/A	N/A	
	1	o uru - chocar	- 0/0 - Wi	Fan Tray	Fan-2	operable	operable	on	ok	N/A	N/A	
	I /1	🔺 0/0 - Major	 0/0 - Inf 	Fan Tray	Fan-3	operable	operable	on	ok	N/A	N/A	
	Unacknowledged	V 1/1 - Minor		Fan Tray	Fan-4	operable	operable	on	ok	N/A	N/A	
				Fan Tray	Fan-1	operable	operable	on	ok	N/A	N/A	
		View in Health M	onitoring	Fan Tray	Fan-2	operable	operable	on	ok	N/A	N/A	
	Harduner Statistics			Fan Tray	Fan-3	operable	operable	on	ok	N/A	N/A	
	Hardware Statistics			Fan Tray	Fan-4	operable	operable	on	ok	N/A	N/A	

Hardware Statistics provides the status of key hardware components of the chassis: Security Engine, Power Supply, and Fan.

Gerenciar interfaces

Operações suportadas na guia Interfaces:

- Atualização da interface física
- Criar/Atualizar/Excluir subinterfaces
- Criar/Atualizar/Excluir interfaces EtherChannel
- · Configurações da interface de sincronização
- OIR do módulo de rede
- Interrupção/junção da interface física

Resumo da guia Interfaces

Chassis Manage Cisco Secure Firewall 4215 Three Summary Interfaces	r: 4215_WA_chass at Defense Multi-Instance Supervisor Instances System Configur	SIS O Connected						Save	Cancel
			CON	SOLE MOMT2 MONT1 US8	Network Module 1 1/1 1/2 1/3 1/4 1/2 1/3 1/4 1/5 1/6 1/7 1/8				
							Q, Search Interfa	ces Sync Devic	e Add
Interface Name	Port Type	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC	
Ethernet1/1	Data	WA_instance_1		Detect SFP	Full	Enabled	Yes	Auto	/
Ethernet1/2	Data	WA_instance_1		Detect SFP	Full	Enabled	Yes	Auto	/
Ethernet1/3	Data			Detect SFP	Full	Disabled	Yes	Auto	/
C Ethernet1/4	Data			Detect SFP	Full	Disabled	Yes	Auto	/
Ethernet1/5	Data			Detect SFP	Full	Disabled	Yes	Auto	/

A página inicial da guia Interfaces mostra todos os tipos de interfaces que são gerenciadas para um chassi, como interfaces físicas, subinterfaces e subinterfaces EtherChannel e EtherChannel.

Modificar configurações de interface física

Estes atributos de uma interface física podem ser atualizados:

- Estado (Habilitado/Desabilitado)
- Tipo de porta (dados | Compartilhamento de dados)
- Admin Duplex
- Velocidade do administrador
- Negociação automática

Edit Physical Interface		0
Interface ID		
Ethernet1/1		Enabled
Port Type		
Data	~	
Admin Duplex		·
Full	\sim	
Admin Speed		
Detect SFP	~	
Admin FEC		e.
Auto	\sim	
Auto Negotiation		
		Cancel OK

Gerenciar Subinterface

Selecione a opção de sub-interface no botão Add para adicionar uma nova interface.

Estes atributos de uma subinterface podem ser modificados:

- Interface pai
- Tipo de porta (dados / compartilhamento de dados)

- ID da subinterface
- ID da VLAN

Admin FEC Auto	Sub Interface EtherChannel Inter
Auto	
	?
~]
~	
	_
	(1-4294967295)
	(1-4094)
	Cancel OK

Gerenciar EtherChannel

Para criar uma nova interface EtherChannel, use a "interface EtherChannel" no botão Add.

Os atributos que podem ser configurados para um EtherChannel são:

• ID do EtherChannel

- Tipo de porta (dados/ compartilhamento de dados)
- Interfaces de membro
- Velocidade do administrador
- Admin Duplex
- Modo LACP
- Taxa de LACP
- Negociação automática

Auto Yes Add EtherChannel Interface Interfaces Configuration EtherChannel ID: (1-48) Data Select Member Interface(s) Available Interfaces (7) Ethernet1/1	Enabled	Admin FEC Auto	dd EtherCha Interfaces	Sub Inte EtherCh	erface hannel Inter	face	Ø
Yes Add EtherChannel Interface Interface Configuration EtherChannel ID: (1-48) Port Type Data Select Member Interface(s) Available Interfaces (7) Ethernet1/1	Enabled	Auto	dd EtherCha Interfaces	annel Interface	/		Ø
Add EtherChannel Interface Interfaces Configuration EtherChannel ID: (1-48) Image: Configuration Port Type Image: Configuration Data Value Select Member Interface(s) Available Interfaces (7) Ethernet1/1 Image: Configuration	Enabled	Ad	dd EtherCha	onnel Interface			0
Interfaces Configuration EtherChannel ID: (1-48) Port Type Data v Select Member Interface(s) Available Interfaces (7) Ethernet1/1	Enabled	Ad	dd EtherCha	onnel Interface			Ø
Port Type Data Select Member Interface(s) Available Interfaces (7) Ethernet1/1	Enabled		Admin Duplex	Configuration			
Port Type Data Select Member Interface(s) Available Interfaces (7) Ethernet1/1		4	Admin Duplex				
Data Select Member Interface(s) Available Interfaces (7) Ethernet1/1		i l â	Authin Duplex				
Select Member Interface(s) Available Interfaces (7)			Full		~		
Available Interfaces (7)		A	Admin Speed				
Ethernet1/1	Selected Interfaces (0)	E P	1Gbps		~		
			LACP Mode				
			Active		~		
Ethernet1/2			LACP Rate				
Ethernet1/3	1		Default		~		
Ethernet1/4	J		Auto Negot	tiation			
Ethemet1/4							
Ethernet1/5						Cancel	OK
Ethernet1/6						Cancer	OR

Configurações do Dispositivo de Sincronização

Há casos em que a configuração do FMC e a configuração do dispositivo podem sair de sincronia. Um caso é quando um usuário remove ou insere um netmod. O dispositivo de sincronização pode ser feito nesses casos.



Suporte A Hot Swap/Break-Out Netmod

A opção "Hot Swap", usada em seus documentos, é conhecida como Inserção e Remoção Online ou OIR em outra documentação interna.

Há uma implantação imediata ao Habilitar/Desabilitar o Módulo de Rede ou Interromper ou Unir interfaces. O modo de várias instâncias é igual ao 4200 Series no modo nativo.



O FMC compara a resposta recebida com a configuração atual e, em seguida, cria a notificação de alteração de interface para confirmação do usuário.

4200 nativo suporta EPM Hot Swap e Breakout

O EPM OIR e o Breakout já são suportados no modo autônomo e nativo do Secure Firewall 4200 Series autônomo.

Documentação do 4200 Series EPM OIR e Breakout FMC:

<u>https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200-install/m-overview.html</u>

OIR: Habilitar/Desabilitar Confirmação do EPM

Quando o usuário alterna para habilitar o módulo, um aviso é exibido para garantir que este não seja um clique acidental.



Ativação Completa do EPM: Notificação de Interface Recebida

- Ao habilitar um EPM, novas interfaces são associadas ao dispositivo.
- O CVP recebe a notificação sobre as interfaces associadas.
- No FMC, o usuário deve aceitar as alterações.

Esta captura de tela mostra a opção de ver as interfaces associadas:

System Config	guration						
		CONSOLE unknown USB	etwork Module 1 1/1 1/2 1/3 1/4 1/5 1/2 1/3 1/4 1/5 1/2 1/1 1/1 1/12 1/1 1/2 1/1 1/11 1/12 1/1	1/6 1/7 1/8	w more. Network Module 2 () 2/1 2/2 2/3 2/4 () () () () () () () () () () () () () (Click to check interface changes	
20	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Ni Yes	

Notificação de Alteração da Interface do EPM

A página de listagem de interfaces lista as interfaces que são adicionadas quando o EPM está habilitado. Clique para saber mais inicia a caixa de diálogo Alterações de interface.

Clique para saber mais não está disponível após salvar.

System Cont	figuration		-		
		Interface Changes	A Interface configuration has	changed on der ice. Click to know more.	Shows interface
		The following interface c changes.	hanges have been detected. Cl	neck if there is any impact on current configuration and accept	the enable
		Interface Name Ethernet2/1/1	Type PhysicalInterface	Change Description Interface is associated	operation
20	Instances	Ethernet2/1/2	PhysicalInterface	Interface is associated	
CI	lick Validate	e and	PhysicalInterface	Interface is associated	
CI	lick Accept	Changes	PhysicalInterface	Interface is associated	
				Close Accept Change	

Página Opções de quebra/junção no chassi

System Configuration							
	CONSOLE unknown USB	etwork Module 1 1/1 1/2 1/3 1/4 1/5 1/ 1/2 1/3 1/4 1/5 1/ 1/4 1/5 1/1 1/2 1/3 1/1 1/4 1/5 1/1 1/12 1/13 1/1	6 1/7 1/8	Network Module 2 () 2/1 2/2 2/3 2/4 () () () () () () () () () () () () () (Break option
pe Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Q. Search Auto Negotiation	Interfaces Admin FEC	Sync Device Add
		Detect SFP	Full	Disabled	Yes	Auto	~
		Detect SFP	Full	Enabled	Yes	Auto	/
		Detect SFP	Full	Enabled	Yes	Auto	/
		Detect SFP	Full	Disabled	Yes	Auto	
		Detect SFP	Full	Disabled	Yes	Auto	
		Detect SFP	Full	Disabled	Yes	Auto	
		Detect SFP	Full	Join	Yes	Auto	
		Detect SFP	Full	option	Yes	Auto	→ >+
		Detect SFP	Full	option	Yes	Auto	

O assistente de confirmação de interrupção da interface é aberto quando a opção de interrupção é acionada. Interface break out is immediate operation and it will be executed instantly on device without needing deployment

Break operation splits the port to multiple ports, Are you sure you want to continue?

Ethernet2/2will break in following interfaces.

Interface Break	Resulting Interface	Admin Speed
	Ethernet2/2/1	10G
Ethernet2/2	Ethernet2/2/2	10G
(Admin Speed:40G)	n Speed:40G) Ethernet2/2/3	
	Ethernet2/2/4	10G



A notificação de atualização da interface fica visível na página do chassi após a confirmação da interrupção da interface.

			 Click on the "Click to know more" link to notice the interface changes 				
System Configuration							
		▲ Interface configuration has changed on device. Click to know more.					
		CONSOLE unknown USB	Network Module 1 1/1 1/2 1/3 1/4 1/5 1/6 1/1 1/2 1/3 1/4 1/5 1/6 1/1 1/2 1/3 1/1 1/1 1/12 1/13 1/1	1/7 1/8 2/1 2/1 1/15 1/15 1/16	vork Module 2		
pe	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Ne	
			1Gbps	Full	Enabled	Yes	
			1Gbps	Full	Enabled	Yes	

Alterações de interface após quebra/junção

Ao clicar em Aceitar alterações, essas interfaces ficam disponíveis no FMC para serem usadas:

System Configuration	n					
			Interface configuration ha	s changed on device. Click to kno	w more.	
						Shows interface
		Interface Changes				changes after the
		The following interface char changes.	nges have been detected. C	Check if there is any impact on cur	rent configuration and accept	break operation
		Interface Name	Туре	Change Description		
		Ethernet2/1	PhysicalInterface	Interface is deleted	· · ·	
pe	Instances	Ethernet2/1/1	PhysicalInterface	Interface is associated		
		Ethernet2/1/2	PhysicalInterface	Interface is associated		
		Ethernet2/1/3	PhysicalInterface	Interface is associated		
					Close Accept Changes	
			1Gbps	Full	Disabled	

Impacto de alterações de interface na instância

Change	Behavior
Change a dedicated interface to shared	No validation error
Change a shared interface used in multiple instance to dedicated	Validation error will block the change
Disable of Network module with interfaces assigned to Instance	No validation error during the disable operation, but error will be thrown in case user tries to accept the notifications without removing the assignment from the instance
Break/Join of interfaces assigned to instance	 Validation error will be thrown to initiate such operation User needs to unassign the interfaces from the Logical Device before initiating Break/Join operation

Gerenciamento de instâncias

O Gerenciamento de Instâncias permite:

- Exibir todas as instâncias de FTD existentes e seus detalhes em um dispositivo 4200 Series (modo MI).
- Crie/Atualize instâncias de FTD com o núcleo da CPU e a versão do software desejados.
- Excluir uma instância de FTD existente.

- Permite que o usuário escolha políticas de FTD Política de acesso e política de Configurações de plataforma para a instância de FTD.
- Registre automaticamente a instância do FTD no FMC quando estiver online.

View I	By: Group ▼ I (1) ● Error (0) ● Warning (0) ◎ Offline (0)	Normal (1) Oeploy	vment Pendii	ng (0) • Upgrade (0)		٩	Search Device	Add 🔻
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	e List Report
	V Ungrouped (1)							
	4215_WA_Chassis 192.168.1.80	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	/1
ick	ick 'Manage' to view 4200 Series (MI mode) Chassis overview							

Criar uma instância

Inicie o assistente clicando em Adicionar instância.



Etapa 1. Contrato:



Etapa 2.

• Fundamentos da configuração da instância:

Add Instance (1) Agreement (2) Instance Configuration	3 Interface 4 Device 5 Summary Assignment Management	Step 2 in instance creation wizard is to configure FTD instance.
Display Name * WA_instance_1 Device Version * 7.6.0.1208 ~ IPv6 Both	Permit Expert mode for CLI Resource Profile* Default-Small +	Display name of FTD instance. FMC lists the device with the same name as on listing page.
IPV4 Management IP* 192.168.1.81 Network Mask* 255.255.255.0 Network Gateway* 192.168.1.254 Search Domain FQDN	DNS Servers Device SSH Password*	Allows configuring core allocation for this FTD instance. You can pick a pre-defined resource profile (Default-Small, Default-Medium, or Default-Large) or make a new one. Use the '+' icon to define a custom resource profile object.
Firewall Mode * Routed	Confirm Password* Show Password Cancel black reakt	FTD version and build number. In 7.6.0, only possible version will be

• IPs de Configuração de Instância:

Add Instance		Θ	Allows user to configure IPv4, IPv6 or Both IPv4
Agreement Agreement Configuration	3 Interface 4 Device Assignment Management	rt	and IPv6 management IP address for FTD instance. Customer will be able to SSH to FTD device using
Display Name * WA_instance_1	Permit Expert mode for CLI		this management IP address
Device Version * 7.6.0.1208	Resource Profile *	+	IPv4 IPv6 Both
IPv4 IPv6 Both			Management IP*
IPv4			2001:a00::192:168:1235
192,168,1,81			Prefix*
Network Mask *			112
255.255.255.0			Network Gateway*
Network Gateway*		·	2001:a00::192:168:1240
192.168.1.254			
Search Domain	DNS Servers	1	IPv4 IPv6 Both
FQDN	Device SSH Password *	,	IPv6 Management IP* Management IP*
)	192.168.1.81 2001:a00::192:168:1235
Firewall Mode *	Confirm Password *		Network Mask* Prefix*
Routed]	255.255.255.0 112
	Show Password		Network Gateway* Network Gateway*
		Capacil Rask Maut	192.168.1.254 2001:a00::192:168:1240
		Cancel Back Next	

Etapa 3. Atribuições de interface:

Add Instance 1) Agreement 2) Instance	Interface 4 Device 5 Summary Assignment	×	Step 3 allows you to assign interfaces to FTD instance.
Available Interfaces (14) Ethernet1/1 Ethernet1/3	Selected Interfaces (2) Ethernet1/2 Ethernet1/4	10 10	Lists all available physical, sub-interfaces and port-channel interfaces.
Ethernet1/5 < Ethernet1/5.11 <	0	1 +	Lists all interfaces selected for this instance.
Ethernet1/5.12 * Ethernet1/9 Ethernet1/10 Ethernet1/11 Ethernet1/12	o o o o o o o o o o o o o o o o o o o	4	Bulk add all and remove all interfaces. Moves all available interfaces as selected interfaces and vice-versa.
Ethernet1/13 Ethernet1/14 Ethernet1/15 Ethernet1/16		4	Delete icon allows you to remove interface from the Selected to Available lists.
Port-channel1	ť	+	Add icon '+' allows you to add an available interface as selected interface.
	Carel Bat	Mart	A share icon Indicates the interface is shared.

Etapa 4. Gerenciamento de dispositivos:

Add Instance	Step 4 allows to assign default access policy, platform setting, device group and choose smart license for FTD.
1 Agreement (2) Instance (3) Interface (4) Davice (5) Summary	
Device Group Select Access Control Policy*	Select an existing device group. FTD instance will be part of the group once online.
Policy1 Platform Settings Select Smart Licensing Z Carrier	Select default access policy. The '+' icon allows creation of a new access policy. It is mandatory to assign an access policy.
Maiware Defense IPS URL URL	Select default platform settings policy. The '+' icon allows creation of a new chassis platform setting policy. It is not mandatory.
	Select smart license(s) applicable for FTD instance.



Etapa 5. Resumo:

Add Instance	(2) Instance (3) In Configuration	terface (4) Device (3) Summary ssignment Management	Ø 	Last step towards creating an FTD instance. Summary tab allows you to review and edit configuration before staging it. (Final step is Deploy.)
Instance Configuration Name: Version: Resource Profile: IP: Mask: Gatework: Mode: Password: FQDN:	WA_instance_1 7.6.0.1208 Default-Small 192.166.1.81 255.255.255.0 192.168.1.254 routed *****	Device Management - Tris into is required only during instance creat Access Policy: Policy1 Device Group: Putoform Policy; Licenses: Carrier, Malware Defense		Each tile summarizes sections of configuration performed in previous steps of the wizard.
DNS Servers: Search Domain: Expert Mode: Interface Assignment - 2 dec	disabled	Port Type		Edit icon in each tile will navigate user to respective section of the wizard, allowing them to edit configuration.
Ethernet1/1 Ethernet1/2		DATA DATA		
		Cancel Back	Save	Final step is to click 'Save'. Configuration will be staged in FMC.

Para concluir a configuração, Salvar e Implantar.

Chassis Manager: 4215_WA_Chass Sizeo Secure Firewall 4215 Threat Defense Multi-Instance Supervisor Immary Interfaces Instances System Configura Name Version Res di WA_Instance_1 7.6.0.1208 Defat Step 2. Click on Def configuration in FM Firewall Management Center Or Chassis Manager: 4215_WA_Chass Cicco Secure Firewall 4215 Threat Defense Multi-Instance Supervisor Instance configuration has changed. A deployment in Summary Interfaces Instances System Configuration	tion Connected Topology to push the staged C to Chassis. Perview Analysis Policies Sis Connected Topology to push the staged C to Chassis.	Management Ga 192.168.1.254	teway Licenses the Carrier,	Vou have unst policy 1. Click on the changes on the Policy 1 Policy Q Q	Save button to sa chassis. N.A	Cancel
Name Version Rest	erview Analysis Policies	Management Ga 192.168.1.254	s Integration	Policy1	Save button to sa chassis. NA	ave ✓∎ securit ancel
Name Version Resident of the second	erview Analysis Connected	Devices Object	s Integration	Policy Q e Advan	Save button to second chassis. N.A	SECUR
de WA_Instance_1 7.6.0.1208 Defait Step 2. Click on Defait Step 2. Click on Defait Step 2. Click on Defait Click on Defa	at-Small 192.168.1.81	192.168.1.254	s Integration	Policy1	N.A ☆ @ admin ~ damin hered Deploy All	the SECUR
Step 2. Click on De configuration in FM Firewall Management Center Chassis Manager: 4215_WA_Chas Cisco Secure Firewall 4215 Threat Defense Multi-Instance Supervise Instance configuration has changed. A deployment is ummary Interfaces Instances System Configu	ploy to push the staged C to Chassis. erview Analysis Policies	Devices Object	s Integration	Deploy Q 🔮 Advan	☆ @ admin ~ 행 nced Deploy All	to SECUR
Step 2. Click on Deconfiguration in FM Configuration in FM Firewall Management Center Chassis Manager: 4215_WA_Chas Citics Secure Firewall 4215 Threat Defense Multi-Instance Supervise Instance configuration has changed. A deployment is ummary Interfaces System Configuration	erview Analysis Policies	Devices Object	s Integration	Deploy Q 🚱	추 🕢 admin ~ 해영	ter SECUR
Firewall Management Center Chassis Manager: 4215_WA_Chas Sisco Secure Firewall 4215 Threat Defense Multi-instance Superviso A Instance configuration has changed. A deployment i mmary Interfaces Instances System Configu	rerview Analysis Policies	Devices Object	s Integration	Deploy Q 💕	갖 😧 admin ~ 해요 nced Deploy Deploy All	tancel
Firewall Management Center Chassis Manager: 4215_WA_Chas isco Secure Firewall 4215 Threat Defense Multi-Instance Superviso Instance configuration has changed. A deployment i mmary Interfaces Instances System Configu	erview Analysis Policies	Devices Object	s Integration	Deploy Q 🤣	🔅 🕢 admin 🗸 🖓	ancel
Firewall Management Center Chassis Manager: 4215_WA_Chas State Secure Firewall 4215 Threat Defense Multi-Instance Supervise Instance configuration has changed. A deployment is immary Interfaces Instances System Configu	erview Analysis Policies	Devices Object	s Integration	Deploy Q 🚱		ancel
Chassis Manager: 4215_WA_Chas Disco Secure Firewall 4215 Threat Defense Multi-Instance Supervise Instance configuration has changed. A deployment in Immary Interfaces Instances System Configu	SSIS Connected	٩		Advan	nced Deploy Deploy All	ancel
Instance configuration has changed. A deployment i Immary Interfaces Instance System Configuration	r					
Instance configuration has changed. A deployment is immary Interfaces Instances System Configu			4215_WA_Chassis	I R	ady for Deployment	
immary Interfaces Instances System Configu	s required.					
	ration					
Name Version Re	source Profile Management IP	Manag				istance
	ault-Small 192.168.1.81	192.16				i i
		0 1	device is available for deploymer	nt	12 O	_
						_
			Step 3. Select th	he device and clip	ick on Deploy	
				eploy' to review t	the changes	

Registro automático de uma instância de FTD após a implantação bem-sucedida:
Chassis Manager: 421 Cisco Secure Firewall 4215 Threat Defense M	5_WA_chas	SIS Connected						Dismiss all notifications
Summary Interfaces Instances	System Configu	ration					6	Chassis
Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy	Ľ	4215_WA_chassis WA_instance_1: provisioning
➤ C v starting v_1	7.6.0.1217	Default-Small	192.168.1.81	192.168.1.254	Carrier,	Pol	Se	Chassis 4215_WA_chassis WA_instance_1: installing
On successf transition fro auto-registra listed in the o user on prog	ul depl m offlir ation w device ress of	oyment, ne to stai ill kick in listing pa f instanc	FTD instar rting, and, and FTD ir age. Task N e creation	nce will boo then, onlin nstance wi Manager m and registi	ot up. li e state Il get re essage ration.	nstanc . Once egister es will	e wi e on red a infoi	ll ine, and rm the

Instância registrada no Management Center:

All (2) • Error (1) • Warning (0) • Offline (0)	Normal (1) Deployment F	ending (1)	 Upgrade (0) Snort 3 (1) 			Q. Search Device	Add
laose All						Download I	Device List Re
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
V Ungrouped (2)							
 4215_WA_chassis 192.168.1.80 	Firewall 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	/
WA_instance_1 Snort 3 192.168.1.81 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A	Essentials, Malware (1 more)	None	«Ş	
\mathbf{i}							
FMC Dev	vice Listing F	Page					
Once aut listed on	to-registratic the device li	n is s sting	successful, t page.	the FTD inst	ance get	ts	

Editar uma instância

Clique no ícone do lápis para editar uma instância de FTD:

Chassis Manager: 42 isco Secure Firewall 4215 Threat Defens mmary Interfaces Instanc	15_WA_cha e Multi-Instance Superv es System Confi	ISSIS OCOnnected isor guration						Sat	Cancel
Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy	Q Search	an instance Platform Settings	Add Instance
• WA_instance_1	7.6.0.1217	Default-Small	192.168.1.81	192.168.1.254	Carrier,	Pol		NA	11
									1
Click o	n the p	encil icor	n to open th	ne edit insta	ance dia	aloa.			0

Etapa 1. Editar instância de FTD:

Edit Instance			
Instance Configuration	2) Interface Assignment3) Summary	The Ed	dit Instance dialog is e Create Instance
Display Name * WA_instance_1	Admin State Permit Expert mode for CLI	wizard	l.
Device Version *	Resource Profile *		
7.6.0.1217 ✓ IPv4 IPv6 Both IPv4 Management IP* 192.168.1.81 Network Mask* 255.255.255.0 Network Gateway* 192.168.1.254	Default-Small ~ +	Howey have t display versio	ver, the user does not he option to edit EULA, y name, or device n.
Search Domain	DNS Servers		
FQDN	Device SSH Password *		
Firewall Mode *	Confirm Password *		
Routed	Annexe ·	Click	on the 'Next' button to
	Cancel	Next Contin	terface assignments

Etapa 2. Editar atribuições de interface para uma instância:

Edit Instance

valiable interfaces (7)		Selected Interfaces (2)		
Ethernet1/3	0	Ethernet1/1		\widehat{u}
Ethernet1/4	0	Ethernet1/2		Ω.
Ethernet1/5	0			
Ethernet1/6	0			
Ethernet1/8	0			
Ethernet1/8.10	0			
Port-channel2	-0			
		>>		
		11		

The next step allows the user to modify interface assignments. User can add new interface or remove existing interfaces.

Click on the 'Next' button to view a summary of changes made to the instance

Etapa 3. Resumo da instância de edição:

1 Instance Configurat	ion 2 Inter	ace Assignment 3 Summary	
stance Configuration			
Name:	WA_instance_1		
Version:	7.6.0.1217		
Resource Profile:	Default-Small		
IP:	192.168.1.81		
Mask:	255.255.255.0		
Gateway:	192.168.1.254		
Mode:	routed		
Password:			
FQDN:			
DNS Servers:			
Search Domain:			
Search Domain: Expert Mode: terface Assignment - 2	disabled dedicated and 0 shared interfaces attached	iie	
Search Domain: Expert Mode: terface Assignment - 2 / Name - Ethemet1/1 Ethemet1/2	disabled dedicated and 0 shared interfaces attached	Port Type DATA DATA	

The last step of editing an instance is to view the summary of changes made to the instance.

Each tile has a pencil icon that navigates user to respective section of the edit steps.

Click the 'Save' button to stage the configuration changes in FMC. The user can review and deploy the changes at a later point in time.

Excluir instância

Cis Sum	hassis Manager: 42' co Secure Firewall 4215 Threat Defense mary Interfaces Instance	5_WA_chas Multi-Instance Supervis System Config	SSIS Connected or uration						Sav	e Cancel
								Q Search	an instance	Add Instance
	Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy		Platform Settings	Delete
,	• WA_instance_1	7.6.0.1217	Default-Small	192.168.1.81	192.168.1.254	Carrier,	Pol		N.A	Cancel

Use the Delete option (from the trash can icon) to delete an existing instance.

Deleting an instance will stage the changes in FMC. Clicking delete will not impact device unless configuration saved and then deployed.

Deleting an instance will free up core allocation.

Configuração de SNMP

Navegue até a guia de configuração do sistema para configurar o SNMP:

5
) NMP

Importação/exportação de chassi

Exportar configuração

Navegue para Gerenciar chassis > Configuração do sistema > Importar/exportar:



Importar configuração

Navegue para Gerenciar chassis > Configuração do sistema > Importar/exportar:



O que você precisa saber sobre importação/exportação de chassis

- Todas as configurações existentes no chassi são substituídas pela configuração no arquivo importado.
- A versão do software da plataforma onde a configuração é importada deve ser a mesma da versão exportada.
- O chassi para o qual você está importando a configuração deve ter o mesmo número de módulos de rede instalados quando a exportação foi realizada.
- O chassi onde a configuração é importada deve ter a mesma imagem de aplicativo instalada para dispositivos lógicos.
- As configurações específicas do aplicativo não são exportadas. Somente as configurações

de chassi são exportadas.

• O backup da(s) Instância(s) do FTD deve ser feito separadamente.

Política de configurações da plataforma do chassi

A política de configurações da plataforma do chassi permite que os usuários definam as seguintes configurações específicas da plataforma:

- Sincronização de horário (NTP)
- DNS
- Syslog
- Fuso horário
- O usuário pode criar uma nova política "Configuração da plataforma do chassi" e atribuí-la a vários chassis 4200 Series (modo MI).



Dica: as configurações da plataforma do chassi aplicam-se apenas ao chassi. Se o usuário quiser aplicar as configurações da plataforma às suas instâncias, poderá usar uma Política de configurações da plataforma Threat Defense.

1. Navegue até chassis Platform Settings policy:

Firewall Management Center Overview Analysis Devices / Device Management	Policies	Device	rs Objects	Integration		Deploy	a 🌮	🗘 😡 admin 🗸	esce SECURE
View By: Group •		Dev	ice Management plate Management	VPN Site To Site	Troubleshoot File Download			Migrate Depic	ryment History
All (4) • Error (1) • Warning (1) = Offline (1) • Normal (1) Collacse All	 Deployment Pen 	QoS Plat	form Settings	Dynamic Access Policy	Packet Tracer Packet Capture			Q, Search Device	Add •
Name	Model	Flex	onfig Licates		Snort 3 Profiling Troubleshooting Logs	Access Contro	i Policy	Auto RollBack	
Ungrouped (3)					Upgrade Threat Defense Upgrade				
9192.168.1.80 192.168.1.80	Firewall 4215 Thre Multi-Instance Su				Chassis Upgrade	N/A		N/A	1
Head to the Platform Set	tinas i	na	ae to						

manage your Chassis Platform Settings.

2. Criar Configurações de Plataforma do Chassi:

			Object Management
			Object Wallagemen
			New Policy
			Firepower Settings
Platform Settings	Device Type	Status	Threat Defense Settings
			Chassis Platform Setting
т	ere are no policies created. Add a new Firepower Settings Policy (or) Threat Defense	Settings Policy (or) Chassis Platform Settings Policy	
		1	

'Chassis Platform Settings' was added in 7.4.1.

- To create a new Chassis Platform Settings Policy click on 'Chassis Platform Settings' under 'New Policy' to launch new platform settings dialog.
- When there are no existing platform setting policies, you will see the 'Chassis Platform Settings Policy' link. This is your launch point to create.

New Policy		×
Name* platformSettingsTP	4	Provide a name for the new Chassis Platform Setting Policy.
Description	4	Add a description to new policy
Targeted Devices Select the devices to which you wan Available Chassis	t to apply this policy. Selected Chassis	List of all existing 4200 Series Chassis.
192.168.1.30	Add	Lists all selected Chassis Click on 'Add' button to move a selected chassis
Chassis IP	Cancel Save	Click on 'Save' button to stage new policy in FMC for subsequent deployment.

3. Página Política de Configurações de Plataforma do Chassi:

Enter Description DNS DNS Resolution Settings SSH Specify DNS servers groups. SSH Access List Syslog Time Synchronization DNS Server Groups Add	Policy Assignments (1)
DNS DNS Resolution Settings SSH Specify DNS servers groups. SSH Access List Image: Comparison of the server groups of the server	
Time Zones	
Each platform setting has its own individual tab. Click on a tab to make configuration changes.	Shows the number of 4200 Series (MI mode) Chassis assigned to this policy. (In this screenshot,

Configurações da plataforma do chassi: DNS

Habilite e adicione grupos de servidores DNS na seção DNS da política de configurações da plataforma do chassi:

platformSettingsTP 🖌	You have unsaved changes Cancel Seve
Enter Description	Enable/Disable DNS resolution on the device
SH The Synchronization The Zones Visiog DNS Server Groups dis_serverTP (default) dialog dialog Click 'Add' to Launch Add DNS Server Group dialog Click 'Add' to Launch Add DNS Server Group Click 'Add' to Click 'Add' to Launch Add DNS Server Group Click 'Add' to Click 'Add' to Cli	Add DNS Server Group Select DNS Server Group* dns_serverTP Make as default
Lists of all DNS server groups	Cancel Save
Click on 'DNS' tab to view DNS specific configuration	Click on delete icon to delete an existing DNS server group. Click on edit icon to launch dialog to edit DNS server group.

Configurações da plataforma do chassi: SSH

 Habilite e adicione o servidor SSH na seção SSH da política de configurações da plataforma de chassi:

				Available Algorithms (14)		Selected Algorithms (6)	
\$	SSH Server			Encryption Encryption		~ Encryption	
				aes128-cbc	0	3des-cbc	
Synchronization	Enable SSH Server			aes128-ctr	0	aes256-cbc	
e Zones	Algorithms			aes128-gcm_openssh_com	0	aes256-ctr	
og	Encountion		Click pencil icon	aes192-cbc	0	✓ Key Exchange	
	3des-cbc		to launch 'Add	aes192-ctr	0	curve25519-sha256	
	aes256-cbc		Algonums	aes256-gcm_openssh_com	0	curve25519-sha256_libssh_org	
	aes256-ctr		dialog	chacha20-poly1305_openssh_com	0	✓ Mac	
	✓ Key Exchange		\ I	✓ Key Exchange		hmac-sha-1	
	curve25519-sha256	libesh ora	\	diffie-hellman-group14-sha1	0		
	Mac	_maan_org	A 1	diffie-hellman-group14-sha256	0		
	hmac-sha-1		· ∖ I	ecdh-sha2-nistp256	0		
			· ∖ I	ecdh-sha2-nistp384	0		
	Host Key*	1024	· ∖ I	ecdh-sha2-nistp521	0		
	Volume Rekey Limit	none KB	· \ Ⅰ	~ Mac			
	Time Dekey Limit		· \ Ⅰ	hmac-sha2-256	0		
	Time Rekey Cimi	Minutes	· · · ·	hmac-sha2-512	0		
			· · · ·				
			\ \ \	· · · · · · · · · · · · · · · · · · ·			
			× 1				

• Habilitar e adicionar cliente SSH:

platformSettingsTP Enter Description	/				`	ou have unsaved changes	Cancel Save Policy Assignments (0)		
DNS SSH Time Synchronization Time Zones Syslog	SSH Server Enable SSH Server Algorithms V Encryption adse-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes256-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc aes26-cbc	Ribssh_org 1024 none none	KB Minutes	SSH Client Strict Host Keycheck Algorithms ~ Encryption a en 192-ctr ~ Key Eschange curve 25519-sha25 curve 25519-sha25 Volume Rekey Limit Time Rekey Limit	enable	SSH Client			
						Strict Host Key Algorithms V Encryption aes192	ycheck n 2-ctr	þisable ✓ disable enable prompt	

Configurações da plataforma do chassi: lista de acesso SSH

Esta guia aparece somente após a ativação do SSH na seção SSH das configurações da plataforma do chassi.

• Criar lista de acesso SSH:

		Available Network Objects (13)	+	Selected Network Objects (2)
	SSH Access List	Q. Search Network Objects		Remove A
4	SSH Access will be allowed to the configured networks	any	0	any-ipv6
Access List	Network List	any-ipv4	0	192.168.1.238
log	Click pencil icon to	IPv4-Benchmark-Tests	0	
e Synchronization	add, modify, or	IPv4-Link-Local	0	
e Zones	delete network or	IPv4-Multicast	0	
	network objects	IPv4-Private-10.0.0.0-8	0	
	for chassis	IPv4-Private-172.16.0.0-12	0	
	access	IPv4-Private-192.168.0.0-16	0	
		IPv4-Private-All-RFC1918	0	
		IPv6-IPv4-Mapped	0	
		IPv6-Link-Local	0	
		IPv6-Private-Unique-Local-Addresses	0	
		IPv6-to-IPv4-Relay-Anycast	0	
	By default, SSH access is denied unless you add a network to the list			Enter IP Host or Network Add
		 Only Network Objects of type 'Host' and 'Network' 	ork' are supported.	Range' and 'FQDN' objects are not supported
		J		Cancel Ad
		•		

• Adicione objetos de rede à lista de acesso SSH:

specific configuration

R. Search Network Objects Remove All any any-ipv6 any-ipv4 92168.1.238 Pv4-Benchmark-Tests 92 Pv4-Link-Local 9 Pv4-Private-100.0.0-8 9 Pv4-Private-102.160.0-12 9 Pv4-Private-122.168.0-16 9 Pv6-IPv4-Napped 9 Pv6-IPv4-Mapped 9 Pv6-Ink-Local 9	vailable Network Objects (13)	+ -	Selected Network Objects (2)		
any any-ipv6 any-ipv6 192.168.1.238 2 Pv4-Benchmark-Tests Pv4-Link-Local Pv4-Miticast Pv4-Private-100.0.0-8 Pv4-Private-102.160.0-12 Pv4-Private-102.160.0-16 Pv4-Private-101.2.168.0-16 Pv6-Ipv4-Mapped Pv6-Ipv4-Mapped Pv6-Ipv4-Mapped Pv6-Ipv4-Relay-Anycast Enter IP Host or Network. Add	Search Network Objects			Remove All	
any-ipv4 192.168.1.238 2 IPv4-Benchmark-Tests IPv4-Link-Local IPv4-Multicast IPv4-Private-100.0.0-8 IPv4-Private-102.168.00-16 IPv4-Private-102.168.00-16 IPv4-Private-1012.168.00-16 IPv6-IPv4-Mapped IPv6-IPv4-Mapped IPv6-IPv4-Relay-Anycast Enter IP Host or Network Add	any	0	any-ipv6	a a	
Pv4-Benchmark-Tests Implementation IPv4-Link-Local Implementation IPv4-Multicast Implementation IPv4-Private-10.0.0.0-8 Implementation IPv4-Private-102.160.0-12 Implementation IPv4-Private-102.168.00-16 Implementation IPv4-Private-102.168.00-16 Implementation IPv6-IPv4-Napped Implementation IPv6-Ink-Local Implementation	any-ipv4	0	192.168.1.238		
Pv4-Link-Local Implementation IPv4-Multicast Implementation IPv4-Private-10.0.0.0-8 Implementation IPv4-Private-122.168.00-12 Implementation IPv4-Private-123.168.00-16 Implementation IPv4-Private-121.168.00-16 Implementation IPv6-Inkv4-Mapped Implementation IPv6-Inkv4-Mapped Implementation IPv6-Inkv4-Mapped Implementation IPv6-Inkv4-Relay-Anycast Implementation IEnter IP Host or Network. Add	IPv4-Benchmark-Tests				
Pv4-Multicast Implementation Implementation Implementat	IPv4-Link-Local	0			
IPv4-Private-10.0.0.0-8 IPv4-Private-172.16.0.0-12 IPv4-Private-192.168.0.0-16 IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-IPv4-Mapped IPv6-Private-Unique-Local-Addresses IPv6-Private-Unique-Local-Addresses IPv6-IPv4-Relay-Anycast	IPv4-Multicast	0			
IPv4-Private-172.16.0.0-12 IPv4-Private-192.168.0.0-16 IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast IEnter IP Host or Network.	IPv4-Private-10.0.0.0-8	0			
IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-Private-Unique-Local-Addresses IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast IEnter IP Host or Network.	IPv4-Private-172.16.0.0-12	0			
IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Link-Local IPv6-to-IPv4-Relay-Anycast IPv6-to-IPv4-Relay-Anycast	IPv4-Private-192.168.0.0-16	0			
Pv6-to-IPv4-Relay-Anycast	IPv4-Private-All-RFC1918	0			
Pv6-Link-Local Pv6-Private-Unique-Local-Addresses Pv6-to-IPv4-Relay-Anycast Enter IP Host or Network. Add	IPv6-IPv4-Mapped	ö			
Pv6-Private-Unique-Local-Addresses Pv6-to-IPv4-Relay-Anycast Enter IP Host or Network. Add	IPv6-Link-Local	0			
Pv6-to-IPv4-Relay-Anycast	IPv6-Private-Unique-Local-Addresses	0			
Enter IP Host or Network Add	IPv6-to-IPv4-Relay-Anycast	0			
			Enter IP Host or Network	Add	

- Network objects can be selected by: 1.Choosing from left side pane.
- 2. By creating a new object using the " +" icon.

• Adicionar um novo objeto de rede:

Add Network Objects		
Available Network Objects (13)	+ Selected Network Objects (1)	
Q. Search Network Objects		Remove All
any	Add Network Object	
any-ipv4		
IPv4-Benchmark-Tests	Name*	
IPv4-Link-Local		
IPv4-Multicast	Description	
IPv4-Private-10.0.0.0-8		
IPv4-Private-172.16.0.0-12		
IPv4-Private-192.168.0.0-16		
IPv4-Private-All-RFC1918	Network	
IPv6-IPv4-Mapped	Host Network	
IPv6-Link-Local		
IPv6-Private-Unique-Local-Addresses		
IPv6-to-IPv4-Relay-Anycast		
	Cancel Save	Add
	jork.	
Only Network Objects of type 'Host' and	'Network' are supported. 'Range' and 'FQDN' objects are not supp	orted
		Cancel Add

Only Host and Network types are supported for chassis access list.

Range and FQDN are NOT allowed.

• Exibir objeto(s) de rede:

Available Network Objects (14)	+	Selected Network Objects (1)	
Q Search Network Objects			Remove
any	0	any-ipv6	-
any-ipv4	0		
IPv4-Benchmark-Tests	0		
IPv4-Link-Local	0		
IPv4-Multicast	ò		
IPv4-Private-10.0.0-8	Ó		
IPv4-Private-172.16.0.0-12	0		
IPv4-Private-192.168.0.0-16	0		
IPv4-Private-All-RFC1918	0		
IPv6-IPv4-Mapped	0		
IPv6-Link-Local	0		
IPv6-Private-Unique-Local-Addresses	0		
IPv6-to-IPv4-Relay-Anycast	0		
Test_Object	0	Enter IP Host or Network	Add
Only Network Outputs of type 'Host' and 'Netw	ork' are supported.	Range' and 'FQDN' objects are not supporte	d
			Cancel

After creation of host object, it will be listed in the available network objects.

• Selecionar objeto(s) de rede:

SSH Access List	Add Network Objects				
SSH Access will be allowed to					After selecting
Network List	Available Network Objects (14)	+	Selected Network Objects (1)		Notwork Objects
	Q Search Network Objects			Remove All	-Network Objects
	any	0	Test_Object		uning the "" icon
	any-ipv4	0			using the + icon
	any-ipv6	-0			from available
	IPv4-Benchmark-Tests	0			
	IPv4-Link-Local	0			network objects it
	IPv4-Multicast	0			HELWOIK ODJECIS, IL
	IPv4-Private-10.0.0.0-8	0			will be listed in the
	IPv4-Private-172.16.0.0-12	0			
	IPv4-Private-192.168.0.0-16	0			selected pane.
	IPv4-Private-All-RFC1918	0			
By default, SSH access is c	IPv6-IPv4-Mapped	0			
	IPv6+Link-Local	0			
	IPv6-Private-Unique-Local-Addresses	0			
	IPv6-to-IPv4-Relay-Anycast	0	Enter IP Host or Network	Add	
	Only Network Objects of type 'Host' and 'Network'	ork' are supported. 1	Range' and 'FQDN' objects are not supported		
			(Cancel Add	

Objetos de rede podem ser criados como também mostrado nesta imagem:

Access List Access will be allowed to ork List	Add Network Objects Available Network Objects (14) Q. Search Network Objects	+	Selected Network Objects (1)	Remove All	Host and network
default, SSH access is c	any any-ipv4 any-ipv6 IPv4-Benchmark-Tests IPv4-Jink-Local IPv4-Multicast IPv4-Private-10.0.0.0-8 IPv4-Private-102.168.0.0-16 IPv4-Private-122.168.0.0-16 IPv4-Private-21.RFC1918 IPv6-IPv4-Mapped IPv6-IPv4-Mapped IPv6-Private-Unique-Local-Addresses	O O O O O O O O O O O O O O O O O O O	Test_Object ddress: The address must contain fi 168.1.1.	four octets between 0 and 255, for	objects can also be added directly from here by providing host IP or Network IP.
	Pv6-to-IPv4-Relay-Anycast Only Network Objects of type 'Host' and 'Net	work' are supported. 'F	192.168.1. Range' and 'FQDN' objects are not s	Add supported Cancel Add	

• Exibir objetos de rede adicionados:



Configurações da plataforma do chassi: sincronização de horário

A Sincronização de Tempo pode ser feita de duas maneiras:

- 1. Via NTP do Management Center
- 2. No servidor NTP personalizado

Do NTP do Management Center

Firewall Management	t Center Overvi	ew Analysis	Policies	Devices	Objects	Integration				Deploy Q	e o o	admin • esce SECURE
platformSettingsTP 🖌	,											Cancel Save Policy Assignments (0)
DNS SSH Time Synchronization	 Via NTP from Mana Use Custom NTP S 	gement Center										
Time Zones Syslog	NTP Servers											
Time Syr	nchroniz	zatior	ı car	ו be	ach	nieveo	d via N	TP				
from Mar	nageme	ent Ce	ente	r or	usir	ng a d	custom	n NTF	P Serv	rer		

No servidor NTP personalizado

platformSettingsTP <		You have unsaved changes Cancel Save Policy Assignments (0)
DNS SSH Via NTP from Management Center Time Synchronization Use Custom NTP Server Time Zones Syslog NTP Servers Add test		
	Add NTP Server	×
	Select NTP Server*	► + New Server
Click on Add and select from the available NTP Server to Use Custom NTP		Cancel Add

Configurações da plataforma do chassi: fusos horários

Definir fusos horários:

D

		Very hours uncounted alternative Council Council	
platformSettingsTP /		Tou nave unsaved changes Cancel	-
Enter Description		Policy Assignments (0))
DNS SSH Time Synchronization Time Zones	Time Zone: (UTC-12:00) Etc/GMT+12 v If no Time Zone is selected, Time Zone will be UTC Time Zone (UTC + 00:00).		
Syslog		Time Zone:	
		(UTC-12:00) Etc/GMT+12 🗸	
		(UTC-12:00) Etc/GMT+12	
		(UTC-11:00) Etc/GMT+11	í.
		(UTC-11:00) Pacific/Midway	
		(UTC-11:00) Pacific/Niue	
		(UTC-11:00) Pacific/Pago_Pago	
		(UTC-11:00) Pacific/Samoa	
		(UTC-11:00) US/Samoa	
efault time zo	ne applied will be UTC + 00:00	(UTC-10:00) America/Adak	
		(UTC-10:00) America/Atka	
		(UTC-10:00) Etc/GMT+10	

Configurações da plataforma do chassi: Syslog

• Guia Destinos locais de Syslog:

platformSettingsTP /			Cancel Save
DNS SSH Time Synchronization Time Zones Syslog	Local Destinations Remote Destinations Local Sources Console Critical Critical Monitor Critical Critical		Policy Assignments (0)
	Level Critical V	Emergencies	~
	Endle Admin State	Emergencies	
	Size* 4194304 Bytes	Alerts	
		Critical	

Guia Destinos remotos de Syslog:

					Emergencies 🗸	
					Emergencies	
					Alerts]
Enter Description	/				Critical	
DNS	Local Destinat	tions Remote Destination	ons Local Sources		Errors	
Time Synchronization	Server1	Admin State			Warnings	
Syslog	Level	Critical	V		Notifications	
	Hostname*	cisco.staging.cisco.com			Information	
	Facility	Local7	×		Debugging	
	Server2	Admin State		Local7 🗸		J
	Level	Critical	~	Local0		
	Hostname*		*	Local1		
	Facility	Local7	~	Local2		
	Enable	Admin State		Local3		
	Level	Critical	~	Local4		
	Hostname*	1		Local5		
	Facility	LOCAI/	~	Local6		
Maximum of three servers	s can be	configured ur	nder Remote Destinations			
				Local		

• Guia Origens Locais de Syslog:



Configurações da plataforma do chassi: salvar e implantar

Firewall Management Center Deploy Q 🔕 🔅 🚱 admin 🗸 👘 SECURE Overview Analysis You have unsaved changes Cancel Save Chassis_Policy / Enter Description Policy Assignments (1) DNS SSH Access List SSH Access will be allowed to the configured networks SSH A Network List / any-ipv4 Test_Object 192.168.1.1 By default, SSH access is denied unless you add a network to the list.

Salve as alterações de configuração da plataforma do chassi e implante:

Now, save the changes which has all the platform settings. Chassis will go for pending deployment.



Cancelando o registro do chassi

Para cancelar o registro do chassi no FMC, navegue até Devices > Device Management > delete.

View By: Group +					Migrate Dep	ployment History		
All (1) • Error (0) • Warning (0) • Offline (0)	Normal (1) Deployment Pendi	ng (0) • Upgrade (0)		Q	Search Device	Add 👻		
Collapse All Download Device List Report								
Name	Model Version	Chassis	Licenses	Access Control Policy	Auto RollBack			
Ungrouped (1)								
4215_WA_Chassis	Firewall 4215 Threat Defense Multi-Instance 7.6.0 Supervisor	Manage	N/A	N/A	N/A	Delete		
						Health Monitor Troubleshoot Files		
Click 'Delete' to unregister 4200 Ser mode) device from FMC	ies (MI							

Converter de Várias Instâncias para o Modo Nativo

Atualmente, o FMC só oferece suporte à conversão de Nativo para Várias Instâncias. Consequentemente, para converter um dispositivo de volta ao modo Nativo, o usuário precisa usar a CLI.

Etapa 1: Cancele o registro do chassi no FMC.

Etapa 2: Use este comando CLI para converter o dispositivo 4200 Series para o modo nativo:

firepower-4215# scope system
firepower-4215 /system # set deploymode native

APIs FMC Rest

As APIs REST públicas do FMC estão disponíveis para todas as operações apoiadas pelo FMC.



APIs REST para conversão de nativo em várias instâncias

API POST para verificar se o dispositivo nativo está pronto para a Conversão de Várias Instâncias:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmodereadinesso

Exemplo de solicitação POST JSON:

```
{
   "devices": [
      {
        "id": "DeviceUUID",
        "type": "Device"
      }
   ],
   "conversionType": "NATIVE_TO_MULTI_INSTANCE"
}
```

API POST para disparar conversão nativa única em Várias Instâncias:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmode

Exemplo de solicitação POST JSON:

```
{
"items": [
{
"id": "
```

```
", "displayName": "Sample_Chassis_Name1" } ], "conversionType": "NATIVE_TO_MULTI_INSTANCE" }
```

API POST para disparar conversão em massa nativa em Várias Instâncias:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/operational/switchmode Exemplo de solicitação POST JSON:

```
{
  "items": [
   {
    "id": "
   ", "displayName": "Sample_Chassis_Name1" }, { "id": "
   ", "displayName": "Sample_Chassis_Name2" } ], "conversionType": "NATIVE_TO_MULTI_INSTANCE" }
```

APIs REST para gerenciamento de chassi

POST Adicione um chassi ao centro de gerenciamento:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis

OBTER todos os chassis:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/

OBTENHA um chassi específico pelo uuid:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

Excluir um chassi pelo uuid:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{objectId}

Exemplo de solicitação POST JSON:

```
{
    "type": "FMCManagedChassis",
    "chassisName": "CHASSIS123",
    "chassisHostName": "192.168.xx.74",
    "regKey": "*****"
}
```

APIs REST para gerenciamento de Netmods (módulos de rede)

OBTENHA um módulo de rede pelo uuid:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/networkmodules/{ob

OBTENHA TODOS os módulos de rede:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/networkmodules/

PUT - Edite um Módulo de Rede existente pelo uuid:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/networkmodules/{ob

PUT - Recuperar dados do módulo de rede do FXOS e atualizar o Centro de Gerenciamento:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/operational/syncnetv

Exemplo de resposta GET

```
"type": "Domain"
    }
 },
  "links": {
    "self": "https://u32c01p10-vrouter.cisco.com:32300/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
 },
  "id": "0050568A-3F3F-0ed3-0000-*********,
  "moduleState": "ENABLED",
  "type": "NetworkModule",
  "description": "Cisco FPR 8X1G 8X10G 1RU Module",
  "model": "FPR-3120",
  "operationState": "ok",
  "numOfPorts": 16,
  "slotId": "1",
  "vendor": "Cisco Systems, Inc.",
  "name": "Network Module 1"
}
```

APIs REST para gerenciamento de instâncias

POST Adicione um chassi ao centro de gerenciamento:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/logicaldevices

OBTER todos os chassis:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/logicaldevices

OBTER uma instância específica por uuid:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/logicaldevices/{objections/

PUT - Editar uma Instância por uuid:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/logicaldevices/{objections/
```

Excluir um chassi pelo uuid:

```
/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/logicaldevices/{objec
```

```
{
    "name": "ftd1",
    "operationalState": "string",
    "deviceRegistration": {
        "licenseCaps": [
            "MALWARE",
            "URLFilter",
            "CARRIER",
            "PROTECT"
    ],
        "accessPolicy": {
            "name": "AC Policy name",
            "
            "Action of the second of the secon
```

", "type": "AccessPolicy" }, "deviceGroup": { "name": "DeviceGroup name", "id": "

", "type": "DeviceGroup" } }, "managementBootstrap": { "ipv4": { "gateway": "192.168.xx.68", "ip

```
", "type": "ChassisInterface" }, { "name": "Ethernet2/2.1", "id": "
```

", "type": "ChassisInterface" }], "type": "LogicalDevice" }

APIs REST para gerenciamento SNMP

OBTER uma configuração SNMP por uuid:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/{object

OBTER TODAS as configurações SNMP:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/

PUT - Edite um Módulo de Rede existente pelo uuid:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/snmpsettings/{object

Resposta GET de exemplo:

```
{
    "snmpAdminInstance": {
        "id": "logicalDeviceUuid",
        "type": "LogicalDevice",
        "name": "ftd3"
},
```

```
"id": "snmpsettingsUUID2",
"type": "SnmpSetting"
}
```

Resumo de APIs REST para busca

Esta lista contém informações detalhadas sobre as APIs REST para buscar o resumo:

- · Falhas
- Instâncias
- Inventário
- Interfaces
- Informações do aplicativo

Resumo de falhas GET para um chassi:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/faultsummary

Resposta de exemplo:

```
{
"links": {
"self": "
```

/api/fmc_config/v1/domain/domainUUID/chassis/fmcmanagedchassis/containerUUID/faultsummary?offset=

Resumo de Instâncias GET para um chassi:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/instancesummary

Resposta de exemplo:

```
{
"links": {
"self": "
```

GET Resumo de inventário para um chassi:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/inventorysummary Resposta de exemplo:

{ "links": { "self": "

/api/fmc_config/v1/domain/domainUUID/chassis/fmcmanagedchassis/containerUUID/inventorysummary?off

Resumo da interface GET para um chassi:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfacesummary

Resposta de exemplo:

{ "links": { "self": "

/api/fmc_config/v1/domain/domainUUID/chassis/fmcmanagedchassis/containerUUID/interfacesummary?off

OBTER Informações do aplicativo para um chassi:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}

/inventorysummary

Resposta de exemplo:

```
{
"links": {
"self": "
```

```
/api/fmc_config/v1/domain/domainUUID/chassis/fmcmanagedchassis/containerUUID/appinfo?offset=0&lim
```

APIs REST para gerenciamento de interface

Esta seção tem informações detalhadas sobre as APIs REST para gerenciamento de configuração de interface:

- · URLs a serem usados para modificações de configuração de interface
- URLs a serem usados para Interrupção/Junção de interfaces
- URLs a serem usadas para configurações do Dispositivo de Sincronização

Atualizar interface física

Para suportar a atualização de interfaces físicas, esses URLs foram apresentados.

OBTER todas as interfaces físicas:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/physicalinterfaces

OBTENHA uma interface física específica pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/physicalinterface s/{interfaceUUID}

Atualizar interface pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/physicalinterface s/{interfaceUUID}

O modelo de interface física é semelhante a este:

```
"metadata": {
    "supportedSpeed": "TEN_GBPS,ONE_GBPS,TWENTY_FIVE_GBPS,DETECT_SFP",
   "mediaType": "sfp",
    "sfpType": "none"
    "isBreakoutCapable": false,
    "isSplitInterface": false,
    "timestamp": 1692344434067,
    "domain": {
     "name": "Global",
     "id": "e276abec-e0f2-11e3-8169-*******",
      "type": "Domain"
   }
 },
  "type": "PhysicalInterface",
  "name": "Ethernet2/2",
  "portType": "DATA",
  "adminState": "DISABLED",
  "hardware": {
    "flowControlSend": "OFF",
    "fecMode": "AUTO",
    "autoNegState": true,
   "speed": "DETECT_SFP",
"duplex": "FULL"
 },
  "LLDP": {
    "transmit": false,
    "receive": false
  }.
  }
```

Configurar subinterfaces

Para suportar o gerenciamento de subinterfaces, esses URLs foram apresentados.

OBTER todas as subinterfaces:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces

OBTENHA uma sub-interface específica pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{inter

POST para uma nova sub-interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces

ATUALIZE a interface pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{interfaces/

EXCLUIR uma sub-interface pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/subinterfaces/{inter

O modelo de subinterface se parece com este:

```
{
  "metadata": {
   "isBreakoutCapable": false,
   "isSplitInterface": false,
   "timestamp": 1692536476265,
   "domain": {
     "name": "Global",
     "id": "e276abec-e0f2-11e3-8169-*******",
     "type": "Domain"
   }
 },
  "type": "SubInterface",
  "name": "Ethernet1/3.3",
  "portType": "DATA",
  "subIntfId": 3,
  "parentInterface": {
   "type": "PhysicalInterface",
   "id": "00505686-9A51-0ed3-0000-********",
   "name": "Ethernet1/3"
 },
  "vlanId": 3,
  }
```

Configurar Interfaces EtherChannel

Para suportar o gerenciamento de interfaces EtherChannel EtherChannel, esses URLs foram apresentados.

OBTENHA todas as interfaces etherchannel:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

OBTENHA uma interface etherchannel específica pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

POST para uma nova interface etherchannel:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/etherchannelinterfac

ATUALIZE a interface pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

EXCLUIR uma interface etherchannel pelo uuid da interface:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/etherchannelinter

O modelo de interface EtherChannel se parece com isto:

```
{
  "metadata": {
    "supportedSpeed": "HUNDRED_MBPS,TEN_MBPS,ONE_GBPS",
    "timestamp": 1692536640172,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-********",
      "type": "Domain"
    }
  },
  "type": "EtherChannelInterface",
  "name": "Port-channel45",
  "portType": "DATA",
  "etherChannelId": 45,
  "selectedInterfaces": [
    {
      "type": "PhysicalInterface",
      "id": "00505686-9A51-0ed3-0000-********",
      "name": "Ethernet1/4"
    },
    {
      "type": "PhysicalInterface",
      "id": "00505686-9A51-0ed3-0000-********",
      "name": "Ethernet1/5"
    }
  ],
  "lacpMode": "ON",
  "lacpRate": "FAST"
  "adminState": "DISABLED",
  "hardware": {
    "flowControlSend": "OFF",
    "autoNegState": true,
    "speed": "ONE_GBPS",
    "duplex": "FULL"
  },
  "LLDP": {
    "transmit": true,
    "receive": true
  },
   'id": "00505686-9A51-0ed3-0000-*********"
}
```

Interfaces de interrupção/junção de APIs REST

Para suportar a Divisão/Junção de interfaces no 4200 Series, estes URLs podem ser usados:

GET:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaces/{

Avalia a viabilidade de interrupção/junção para uma interface

POST:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/break

Interrompe uma interface

POST:

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/joinin Une um conjunto de interfaces quebradas

Fluxo REST para quebra de interface

1. Localize o dispositivo de chassi gerenciado do FMC (4200) usando o endpoint fmcmanagedchassis.

GET /api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis

Retorna a lista de dispositivos de chassi gerenciados do FMC junto com dispositivos de Várias Instâncias com detalhes como ID, nome e modelo de cada dispositivo. Escolha os dispositivos "MULTIINSTANCE".

Resposta de exemplo:

```
{
   "id": "fcaa9ca4-85e5-4bb0-b049-*******",
   "type": "FMCManagedChassis",
   "chassisName": "192.168.0.75",
   "chassisMode": "MULTIINSTANCE",
   "links": {
        "self": "https://u32c01p06-vrouter.cisco.com:22512/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
   }
}
```

2. Verifique se a interface tem capacidade de breakout usando o ponto final interfaces/physical interfaces.

A reunião à parte só será possível se "isBreakoutCapable" for verdadeiro e mediaType for QSFP.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

Resposta de exemplo:

```
"domain": {
    "name": "Global",
    "id": "e276abec-e0f2-11e3-8169-*******",
    "type": "Domain"
  }
},
"type": "PhysicalInterface",
"name": "Ethernet2/4",
"portType": "DATA",
"adminState": "DISABLED",
"hardware": {
  "flowControlSend": "OFF",
  "fecMode": "AUTO",
  "autoNegState": true,
  "speed": "DETECT_SFP",
"duplex": "FULL"
},
"LLDP": {
  "transmit": false,
  "receive": false
}.
"id": "00505686-9A51-0ed3-0000-********"
```

3. Na interface, avalie a viabilidade da operação de quebra usando o ponto final de avaliaçãooperação.

GET

}

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaces/{in

Se não houver avisos/erros na resposta, o usuário poderá executar a operação de interrupção.

Resposta de exemplo:

```
{
    "operationType": "BREAKOUT",
    "readinessState": "READY",
    "links": {
        "self": "https://u32c01p06-
vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/chassis/fmcmanagedchassis/19d967e6-ef81-4f2e-b311-
85ff6cef6d3f/chassisinterfaces/00505686-662F-0ed3-0000-
004294969274/evaluateoperation/00505686-662F-0ed3-0000-004294969274"
        },
        "type": "ChassisInterface",
        "id": "00505686-662F-0ed3-0000-004294969274"
    }
```

Se houver erros na resposta, o usuário não poderá executar a operação de interrupção:

```
{
    "operationType": "BREAKOUT",
    "interfaceUsages": [
```

4. Se a interface for habilitada para breakout e o estado de prontidão for "READY", quebre a interface usando o ponto final breakoutinterfaces.

POST

/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational/break

Solicitação:

Resposta:

5. Rastreie a conclusão da tarefa usando o id da tarefa na resposta à interrupção. Defina o status da tarefa como "Notificação de interface recebida".

GET /api/fmc_config/v1/domain/{domainUID}/job/taskstatuses/{objectId}

```
{
 "metadata": {
   "task": {
     "id": "4294969699",
     "links": {
       "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-
     }
   }
 },
 "targetInterfaces": [
   {
     "id": "00505686-662F-0ed3-0000-*******",
     "type": "PhysicalInterface"
   }
 ],
  'type": "BreakoutInterface"
}
{
 "id": "4294969716",
 "type": "TaskStatus",
 "links": {
   "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
 },
 "taskType": "DEVICE_DEPLOYMENT",
 "status": "Interface notification received"
}
```

6. Obtenha as alterações de interface usando o ponto de extremidade chassisinterfaceevents.

GET /api/fmc_config/v1/domain/{domainUID}/chassis/ fmcmanagedchassis/{containerUID}/chassisinterfaceevents

Resposta de exemplo:

```
Ε
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3"
  },
  {
    "change": "Interface is associated",
    "type": "PhysicalInterface",
    "state": "ASSOCIATED",
    "name": "Ethernet2/3/2"
  },
  {
    "change": "Interface is associated",
    "type": "PhysicalInterface",
```

```
"state": "ASSOCIATED",
    "name": "Ethernet2/3/3"
},
{
    "change": "Interface is associated",
    "type": "PhysicalInterface",
    "state": "ASSOCIATED",
    "name": "Ethernet2/3/4"
}
```

7. Se a notificação de interface não for recebida, sincronize o dispositivo usando o ponto de extremidade chassisinterfaceevents e verifique se há alterações pendentes.

POST /api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/ chassisinterfaceevents

Solicitação:

```
{
    "action": "SYNC_WITH_DEVICE"
}
```

Resposta:

```
{
    "action": "SYNC_WITH_DEVICE",
    "hasPendingChanges": true
}
```

8. Quando a notificação for recebida, aceite as alterações usando o ponto final chassisinterfaceevents.

POST /api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/ chassisinterfaceevents

Solicitação:

```
{
    "action":"ACCEPT_CHANGES"
}
```

9. Obtenha todas as interfaces do chassi e localize as interfaces divididas (quebradas) usando o

endpoint de interfaces.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

Uma interface 40G, digamos eth2/2, é dividida em interfaces 4x10G - eth2/2/1, eth2/2/2, eth2/2/3 e eth2/2/4

Fluxo REST para junção de interface

1. Verifique se a interface está quebrada usando o endpoint interfaces/physicalinterfaces.

A operação de junção só será possível se "isSplitInterface" for verdadeiro e mediaType for SFP

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

```
{
  "metadata": {
    "supportedSpeed": "TEN_GBPS,DETECT_SFP",
    "mediaType": "sfp",
    "sfpType": "none"
    "isBreakoutCapable": false,
    "breakoutFactor": "4",
    "isSplitInterface": true,
    "timestamp": 1692541554935,
    "domain": {
      "name": "Global",
      "id": "e276abec-e0f2-11e3-8169-********",
      "type": "Domain"
    }
  },
  "type": "PhysicalInterface",
  "name": "Ethernet2/3/4",
  "portType": "DATA",
  "adminState": "DISABLED",
  "LLDP": {
    "transmit": false,
    "receive": false
 },
  "hardware": {
    "flowControlSend": "OFF",
    "speed": "DETECT_SFP",
    "duplex": "FULL",
    "fecMode": "AUTO"
    "autoNegState": true
 },
   'id": "00505686-662F-0ed3-0001-*********
}
```

2. Avalie a viabilidade da operação Join usando o ponto final de avaliaçãooperation em uma das quatro interfaces de divisão.

GET /api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterfaces/{interfaceUUID}/valuateoperation

• Se não houver avisos/erros na resposta, o usuário poderá executar a operação Ingressar.

• Se houver erros na resposta, o usuário não poderá executar a operação de junção.

```
{
  "operationType": "JOIN",
  "interfaceUsages": [
    {
      "conflictType": "Interface used in EtherChannel Configuration",
      "severity": "ERROR",
      "description": "Interface (Ethernet2/3/4) referred to in Ether Channel Interface (Port-channel32)
    }
 ],
  "readinessState": "NOT_READY",
  "links": {
    "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
 },
  "type": "ChassisInterface",
  "id": "00505686-662F-0ed********************
}
```

3. Se a interface estiver quebrada e o estado de prontidão for "PRONTO", una-se à interface usando o ponto final joininterfaces. Interface_uuid pode ser o id de qualquer uma das 4 interfaces quebradas.

POST/api/fmc_config/v1/domain/{domainUUID}/chassis/fmcmanagedchassis/{containerUUID}/operational

Solicitação:
"type": "JoinInterface" }

Resposta:

```
{
    "metadata": {
        "task": {
            "id": "4294970217",
            "links": {
                 "self": "
```

4. Rastreie a conclusão da tarefa usando o id da tarefa na resposta de junção. Defina o status da tarefa como "Notificação de interface recebida".

GET /api/fmc_config/v1/domain/{domainUID}/job/taskstatuses/{objectId}

Resposta:

```
{
   "id": "4294970237",
   "type": "TaskStatus",
   "links": {
        "self": "https://u32c01p06-vrouter.cisco.com:22542/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169
   },
   "taskType": "SSP_EPM_OIR",
   "message": "Deployment status for 19d967e6-xxxx-xxxx-85ff6cef6d3f: SUCCEEDED",
   "status": "Interface notification received"
}
```

5. Obtenha as alterações de interface usando o ponto de extremidade chassisinterfaceevents.

GET

/api/fmc_config/v1/domain/{domainUID}/devices/devicerecords/{containerUID}/chassisinterfaceevents

Resposta:

```
Ε
  {
    "change": "Interface is associated",
    "type": "PhysicalInterface",
    "state": "ASSOCIATED",
    "name": "Ethernet2/3"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/1"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
    "name": "Ethernet2/3/2"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
"state": "DISASSOCIATED",
    "name": "Ethernet2/3/3"
  },
  {
    "change": "Interface is deleted",
    "type": "PhysicalInterface",
    "state": "DISASSOCIATED",
"name": "Ethernet2/3/4"
  }
```

6. Se a notificação de interface não for recebida, sincronize o dispositivo usando o ponto de extremidade chassisinterfaceevents e verifique se há alterações pendentes.

POST

]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/chassisinterfaceevents

Solicitação:

```
{
   "action": "SYNC_WITH_DEVICE"
}
```

Resposta:

```
{
   "action":"SYNC_WITH_DEVICE",
   "hasPendingChanges":true
}
```

7. Quando a notificação for recebida, aceite as alterações usando o ponto final chassisinterfaceevents.

POST

/api/fmc_config/v1/domain/{domainUID}/devices/devicerecords/{containerUID}/chassisinterfac events

Solicitação:

```
{
    "action":"ACCEPT_CHANGES"
}
```

8. Obtenha todas as interfaces do chassi e localize as interfaces unidas, bem como as outras interfaces, usando o endpoint de interfaces.

GET

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/interfaces

Digamos que a união tenha sido iniciada na interface 10G, digamos eth2/2/1, então uma interface 40G eth2/2 estará disponível na resposta.

Sincronizar APIs REST de Dispositivo

Para suportar a Sincronização do Módulo de Rede e das Interfaces, esses URLs foram apresentados.

POST:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterface events

Com payload

{"action": "SYNC_WITH_DEVICE"} - > Aciona a Sincronização

{"action": "ACCEPT_CHANGES"} - > Aceitar as alterações

GET:

/api/fmc_config/v1/domain/{domainUID}/chassis/fmcmanagedchassis/{containerUID}/chassisinterface events

Lista os eventos alterados gerados

Solução de problemas/diagnósticos

Log FXOS

Se o registro falhar, essas CLIs FXOS podem ser usadas para verificar se os processos sftunnel e sfipproxy estão ativos.

firepower# connect local-mgmt
firepower-4215(local-mgmt)# show processes | include sftunnel grep: (standard input): binary file match
3323 root 20 0 80328 2024 1544 S 0.0 0.0 0:11.53 /opt/cisco/sftunnel/sfipproxy -d -f /etc/sf/sfipproxy.
22066 root 20 0 376880 7140 5944 S 0.0 0.0 0:41.18 /opt/cisco/sftunnel/sftunnel -d -f /etc/sf/sftunnel.

Se estiver usando o console do terminal para a CLI, certifique-se de que a saída de show processes não esteja truncada, definindo a largura do terminal com um valor apropriado usando esta CLI mostrada:

```
firepower-4215(local-mgmt)# terminal width 100
```

Se o processo SFTunnel estiver ativo e em execução, mas o registro estiver falhando, esses comandos podem ser usados para encontrar qualquer motivo potencial para a falha.

Introduziu a nova CLI no FXOS do connect local-mgmt para exibir mensagens de syslog em /opt/cisco/platform/logs/sfmessages

```
firepower# connect local-mgmt
firepower(local-mgmt)# tail-mgmt-log sfmessages
```

Dec 9 18:31:17 firepower Ipc [30483]: add ep: 1,0x5613aa0e2fe8 total = 1 Dec 9 18:31:17 firepower

Registro do CVP

- Se o registro do dispositivo falhar, localize usmsharedsvcs.log e vmssharedsvcs.log neste local e procure a string "CHASSIS DISCOVERY" ou "NATIVE_TO_MULTI_INSTANCE" para encontrar a causa potencial da falha.
 - Além disso, procure em /var/log/action_queue.log e /var/sf/messages problemas de SFTunnel.

- /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
 /var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log
- Se o registro automático do chassi falhar, localize usmsharedsvcs.log e vmssharedsvcs.log e procure a string"CHASSIS DISCOVERY" e "NATIVE_TO_MULTI_INSTANCE" para encontrar a causa potencial da falha.
- Se o registro automático da instância falhar, localize usmsharedsvcs.log e vmssharedsvcs.log e procure a string "MI_FTD_INSTANCE_AUTO_REGISTRATION" para localizar a causa potencial da falha.
- Se houver uma falha de implantação no dispositivo, navegue para Implantar -> Histórico de implantação -> Clique na implantação com falha -> Abrir transcrição. Este arquivo contém o motivo da falha.

Solução de problemas do chassi

O FMC suporta a geração de solução de problemas de chassi (FPRM) na página de gerenciamento de dispositivos.

- Como o dispositivo FTD, há uma opção de solução de problemas disponível para o dispositivo de chassi que gera solução de problemas de chassi e permite que o usuário faça o download do pacote de solução de problemas do FMC.
- Isso coleta o pacote "show tech-support form" (mostrar formulário de suporte técnico) do chassi:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
\sim Ungrouped (2)							
4215_WA_chassis 192.168.1.80	Firewali 4215 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A	N/A	✓ : Delete
WA_instance_1 Snort 3 192.168.1.81 - Routed	Firewall 4215 Threat Defense	7.6.0	N/A	Essentials, Malware (1 more)	Pol	4 ⁰	Health Monitor Troubleshoot Files

Opções de solução de problemas e geração de chassis:



Progresso e download da solução de problemas do chassi:

	Deployments Upgrades \varTheta Health Tasks 🛨 💽 Show Pop-up Notifications 🕕	
	12 total 0 waiting 2 running 0 retrying 10 success 0 failures Q Filter	
 Task Manager messages show the progress of troubleshoot generation. 	Chassis Generate Troubleshooting Files Generate troubleshooting files for 4215_WA_chassis Remote status: Generating troubleshoot files	
 Once completed, the user can download the troubleshoot bundle. 	Deployments Upgrades Image: Health Tasks Image: Tas	is 🚺
	Generate Troubleshooting Files 7m 57 Generate troubleshooting files for 4215_WA_chassis 7m 57 Click to retrieve generated files.	s X

Exemplos de Problemas com Troubleshooting de Passo a Passo

Registro automático de falha de chassi no FMC

Problema: o registro automático do chassi está falhando no FMC.

Resultado esperado:

• Uma vez iniciada a conversão a partir do CVP, espera-se que não seja registrada e que seja registrada automaticamente no CVP.

Resultado real:

· Falha no registro automático do chassi

Solução de problemas

- 1. Verificar conversão:
 - · Verificar se a conversão foi desencadeada no CVP.
 - Faça login no dispositivo e verifique se o dispositivo foi convertido para o modo de contêiner.
 - Execute os comandos para ver se o dispositivo foi convertido:

```
firepower# scope sys
firepower /system # show
Systems:
Name Mode Deploy Mode System IP Address System IPv6 Address
firepower Stand Alone Container 192.168.xx.xx ::
```

2. Verifique o gerenciador de dispositivos:

• Verifique se o gerenciador de dispositivos foi definido corretamente:

```
firepower# show device-manager
Device manager:
Name: manager
Hostname: 10.10.xx.xx
NAT id: 3ab4bb1a-d723-11ee-a694-89055xxxxxxx
Registration Status: Completed
Error Msg:
```

3. Logs a verificar:

3.1. Navegue até /var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log e /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

3.2. Procure as palavras-chave"NATIVE_TO_MI_CONVERSION" e"CHASSIS DISCOVERY" nos arquivos para encontrar o motivo da falha.

Autorregistro de instância no CVP

Problema: o registro automático da instância está falhando no FMC.

Resultado esperado:

 Quando a instância for provisionada pelo FMC, ela deverá ser registrada automaticamente no FMC

Resultado real:

· Falha no registro automático da instância

Solução de problemas

- Verifique se a implantação foi disparada após a criação da instância.
 - Se a implantação não estiver concluída, assegure-se de implantar as alterações no dispositivo.
 - Se houver uma falha na implantação, vá para Histórico de implantação -> Clique em Transcrição. Verifique o motivo da falha, corrija e repita a implantação.
- Verifique se a instância está instalada e se seu estado operacional está online. Você pode usar a página de resumo do chassi para verificar o status do provisionamento da Instância.

		360-2022	09:52 Instances			Live status	at: 1
Name blr_instance1 Operational state online Management IP 192.168.1.88 ^{:52}	Hide details		List of online inst	2 tances	2 Instances Found		
atec Cores used 8 0/0 - Critical 1/1 - Warning .0/0 - Major 0/0 - Info	Up: 1	_	 blr_instance1 blr_instance_2 	online 2 2 online Online	O A Error	0 Ø Offline	

 Verifique se o SFTunnel está ativo e em execução no FTD da instância usando este comando:

ps -ef | grep -i "sftunnel"

• Se o SFTunnel não estiver em execução, tente executar um comando de reinicialização:

pmtool restartById sftunnel

- Navegue até /var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log e /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
- Procure a palavra-chave "MI_FTD_INSTANCE_AUTO_REGISTRATION" no arquivo para encontrar o motivo da falha.

Registro de dispositivo nativo no FMC

Problema: o Native Device Registration está falhando no FMC após a conversão do dispositivo de volta ao modo nativo

- Caso o usuário converta o chassi (modo MI) de volta para o modo nativo, mas se esqueça de excluir o chassi do FMC, o dispositivo fica off-line no FMC.
- Se o usuário tentar registrar novamente esse dispositivo nativo no FMC, o registro falhará.

Solução de problemas

- Verifique se a entrada do chassi foi excluída do FMC antes de converter o dispositivo de volta ao modo nativo.
- Quando a entrada for excluída, tente registrar novamente o dispositivo nativo no FMC.

Referências úteis

• Informações sobre interfaces compartilhadas:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multiinstance-sec-fw/multi-instance-sec-fw.html#shared-interface-scalability-WGUIEF

• 3100 Página de várias instâncias no site de suporte da Cisco:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html

Opções de interface e alta disponibilidade

Opções de interface



Independente ou alta disponibilidade





		l	

Aproveitando as interfaces de gerenciamento duplas

 Como o 4200 no modo nativo, as duas portas de gerenciamento físico são fornecidas para suportar redundância de interface para tráfego de gerenciamento ou para suportar interfaces separadas para gerenciamento e eventos.

- Os dispositivos 9300 e 4100, assim como o 4200 Series, têm interfaces de gerenciamento duplas. A segunda interface de gerenciamento, Gerenciamento 1/2, é destinada a ser usada para eventos.
- No modo de várias instâncias (também conhecido como "contêiner"), você pode configurar essa interface na CLI do Threat Defense em cada instância. Atribua um endereço IP na mesma rede para cada instância.
- Quando no modo de contêiner, cada instância de FTD tem interfaces de Gerenciamento 1/1 e Gerenciamento 1/2 automaticamente atribuídas a ela.
 - A segunda interface de gerenciamento é desativada por padrão.
 - Você não pode configurar o Management1/2 usando o FMC; você precisa configurá-lo através do CLISH FTD (no 9300/4100, que, por outro lado, é feito no FXOS CLI). Use este comando com o tipo de endereço IP, endereço, sub-rede e rota estática desejados:

configure network ipv4 manual 192.168.0.xx 255.255.255.0 192.168.0.1 management1

Informações de rastreamento interno

Functional Spec	EDCS-24403363
Target Process	TP-794577
Addresses Bug(s)	CSCwh98021 WA Conversion
Bugs for this feature are in this Project > Product > Component in CDETS	CSC.content-security > sfims > fmc_mi_ui
Eng Contact(s)	Bhargav Kumar Rasetty (brasetty)

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.