## Configurar a alta disponibilidade no FMC

## Contents

<u>ntrodução</u>
Pré-requisitos
Requisitos
Componentes Utilizados
nformações de Apoio
intes de Começar
Configurar
Configurar o FMC secundário
Configurar o FMC primário
<u>'erificação</u>

## Introdução

Este documento descreve um exemplo de configuração de HA (High Availability, alta disponibilidade) em um FMC (Firewall Management Center, centro de gerenciamento de firewall).

## Pré-requisitos

#### Requisitos

Não existem requisitos específicos para este documento.

#### **Componentes Utilizados**

As informações neste documento são baseadas no Secure FMC para VMware v7.2.5.

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

Os requisitos específicos deste documento incluem:

- Os dois pares do FMC devem estar na mesma versão de software, atualização de regra de intrusão, banco de dados de vulnerabilidades e Lightweight Security Package
- · Ambos os pares do FMC devem ter a mesma capacidade ou versão de hardware
- Ambos os CVP exigem uma licença separada

Para obter um conjunto completo de requisitos, acesse o Guia de administração.



aviso: Se houver uma incompatibilidade nos requisitos listados, você não poderá configurar o HA.

Este procedimento é suportado em todos os dispositivos de hardware.

### Antes de Começar

- · Garantir o acesso do administrador a ambos os FMCs
- · Garanta a conectividade entre interfaces de gerenciamento
- Reserve alguns minutos para revisar as versões de software e garantir que todas as atualizações necessárias sejam feitas

## Configurar

#### Configurar o FMC secundário

Etapa 1. Inicie a sessão na interface gráfica do usuário (GUI) do dispositivo do FMC que assumirá a função de secundário/em espera.



Iniciar sessão no FMC

#### Etapa 2. Navegue até a guia Integração.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	Devices	Objects	Integration	Deploy Q	🥝 🌣 🔞 admin	▼ dialia cisco SECURE
								Reporting
Summary Dashboard (witch dashboard) Provides a summary of activity on the appliance								
Network × Threats Intrusion Events	Status Geo	location QoS	+			Show the Last	1 hour	• II
								Add Widgets
<ul> <li>Unique Applications over Time</li> </ul>	$-\times$	Top Web Applica	tions Seen		$-\times$	Top Client Application	ns Seen	- ×
No Data			No Data				No Data	
No devices registered.			No devices regi	istered.		No	devices registered.	
Click here to register a device.		CI	ck here to registe	er a device.		Click h	ere to register a device	). 
Last undated 3 minutes ann								
enor abarroa o minarco alla		Last updated 3 minutes	ago			Last updated 3 minutes ago		
<ul> <li>Traffic by Application Risk</li> </ul>	- ×	Top Server Appli	cations Seen		$-\times$	Top Operating System	ns Seen	- ×
No Data								

Navegue até a integração

Etapa 3. Clique em Outras Integrações.

Integration	Deploy	Q 🧧	☆	🕜 admin ▼	cisco
SecureX Security Analytics & Lo Other Integrations	gging	Intel Incio Sou	l <b>igence</b> dents rces		
AMP		Elen Sett	nents ings		
AMP Management Dynamic Analysis Conn	nections		-		

Navegue até Outra Integração

#### Etapa 4. Navegue até a guia Alta Disponibilidade.

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Ma	y Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Navegar para Alta Disponibilidade

#### Etapa 5. Clique em Secundário.

Firewall Integration	Manage / Other Integ	ment Center rations / High Availabilit	y Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	۵	🕜 admin 🔻	cisco SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Sm	art Software M	lanager On-Prem						Peer Manager
Select a role for	this Mana	gement Center and	specify peer detai	ls to setup hig	gh availability	y.								
Role For This Firev Standalone (N	vall Manage o High Avail	ment Center: ability)												
O Primary														

Secondary

Inserir informações e selecionar a função desejada para o FMC atual

Etapa 6. Insira as informações do peer Principal/Ativo e clique em Register.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	Peer Manager
Select a role for	this Manag	ement Center and	specify peer detail	s to setup hig	h availability.		
Role For This Firew	vall Managem	ent Center:					
Standalone (No	o High Availal	pility)					
O Primary							
<ul> <li>Secondary</li> </ul>							
Peer Details:							
After Firewall Mana	agement Cen	ter high availability is	configured in virtual of	r cloud environr	ment, each registered	Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Primary Firewall M	anagement C	enter Host:					
10.18.19.31							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register							
† Either host or NAT I	D is required.						



Note: Anote a chave de registro, já que ela será usada no FMC ativo.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?





Note: Certifique-se de que não haja outra tarefa em execução enquanto o HA estiver sendo criado, a GUI será reiniciada.

Etapa 8. Confirme se você deseja registrar o peer principal.



Do you want to register primary peer: 10.18.19.31?





aviso: Todas as informações em Devices/Policy/Configuration serão removidas do FMC secundário assim que o HA for criado.

#### Passo 9. Verificar se o estatuto de CVP secundário está pendente.

Ę	Firewall I Integration /	Managen Other Integra	nent Cer ations / Pee	nter r Manager	Overview	Analysis	Policies	Devices	o Objects	Integration	Deploy	Q	0	🌣 🔞 admin 🔻	cisco SECURE	
	Cloud Services	Realms	Identity	Sources	High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	re Manager On-Prem						
	Host			Last Modif	ied				Status				Sta	ate		
	10.18.19.31			2023-09-	28 13:53:56			ſ	Pending Registratio	n				0	/1	

#### Configurar o FMC primário

Repita as etapas de 1 a 4 no FMC principal/ativo.

Etapa 5. Clique em Primário.

Firewall Mana Integration / Other	gement Center ntegrations / High Availabil	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢ (	admin 🔹	cisco SECURE
Cloud Services Real	ns Identity Sources	High Availability	eStreamer	Host Input C	Client Sn	nart Software M	Manager On-Prem						Peer Manager
Select a role for this N	anagement Center and	I specify peer detai	ls to setup hig	gh availability.									
Role For This Firewall Mar	agement Center: Availability)												
Primary													
<ul> <li>Secondary</li> </ul>													
Peer Details:													
Configure the secondary After Firewall Managemen Secondary Firewall Manag	Management Center with t Center high availability is sement Center Host:	details of the primary b s configured in virtual	pefore registrati or cloud enviror	ion. nment, each re	gistered Fire	wall Threat Def	iense consumes an a	additional Fire	power	MCv D	evice l	license.	
Registration Key*:													
Unique NAT ID:													
Register † Either host or NAT ID is requ	ired.												

### Etapa 6. Insira as informações sobre o FMC secundário e clique em Register.

						Pi	eer Manager
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	
Select a role for	this Manag	gement Center and	specify peer detai	ls to setup hig	h availability.		
Role For This Firev	vall Manager	nent Center:					
Standalone (N)	o High Availa	bility)					
Primary							
<ul> <li>Secondary</li> </ul>							
Peer Details:							
Configure the second After Firewall Man	ondary Mana agement Cer	gement Center with onter high availability is	letails of the primary configured in virtual	before registration	on. ment. each registered	d Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Secondary Firewa	II Manageme	nt Center Host:					
10.18.19.32							
Registration Key*:							
cisco123							
Unique NAT ID:							
Register	ID is required						
F LIGHT HOST OF NALL	is required.						



Note: Utilizar a mesma chave de registro utilizada como FMC secundário.

Etapa 7. Este aviso solicita que você confirme, clique em yes.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?





Note: Verifique se não há outra tarefa em execução.

Etapa 8. Confirme se você deseja se registrar no FMC secundário.

# Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer: 10.18.19.32?





Note: Verifique se não há informações críticas no FMC secundário, pois aceitar esse prompt remove todas as configurações do FMC.

Sincronização entre os inícios Primário e Secundário; a duração depende da configuração e dos dispositivos. Esse processo pode ser monitorado em ambas as unidades.

	Firewall I Integration /	Managen Other Integra	nent Cent ations / High A	er wailability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (	\$	🕜 admin	eisco SECURE
															Peer Manager
Cloud \$	Services	Realms	Identity Sou	irces	High Availability	eStreamer	Host Input	t Client Sr	mart Software M	Manager On-Pre	m				
										Switch Peer R	oles 🗳	Break HA		II Pause Sy	vnchronization
				High ava These oj Databas	ilability operations and perations include file e files synchronization	re in progress. The copy which may t n: 100% of 379MI	e status messa ake time to co 8 transferred	ages and alerts omplete.	on this page are	e temporary. Plea	se check after high	availabilit	ty opera	ions are compl	ete. ×
	Summa	ry						S	ystem Statu	s					
	Status		A Tem	porarily	degraded- high ava	ailability operation p	ns are in rogress.				Local Active - Primary (10.18.19.31)		Stan	Remote dby - Seconda (10.18.19.32)	ary
	Synchron	nization				4	Failed	C	perating Syste	m	7.2.5			7.2.5	
	Active Sy	/stem				10.1	8.19.31	s	oftware Version	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	8.19.32	Μ	lodel	Secur	e Firewall Manag Center for VMwar	ement e	S Mana	ecure Firewall gement Cente VMware	r for



Note: Enquanto a sincronização estiver ocorrendo, espere ver o status como Falha e Temporário degradado. Esse status é mostrado até que o processo seja concluído.

## Verificação

Uma vez concluída a sincronização, a saída esperada é Status Healthy e Sincronização OK.

Firewal Integration	I Manage	ment Center grations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	\$ (	admin	• diala SI
														Peer Man
oud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Cl	lient Sn	nart Software N	lanager On-Prem						
							5	Switch Peer Roles	44	Break H	A	חו	Pause S	ynchronizatio
Summ	nary					S	ystem Statu:	S						
Status				0 H	ealthy			Activ	Local		51	F	emote	lanı
Synchr	ronization				OK OK			(10	.18.19.31)		5	(10	18.19.32)	lar y
Active	System			10.18.	19.31	0	perating System	m	7.2.5				7.2.5	
Standb	by System			10.18.	19.32	S	oftware Versior	n 7.	2.5-208			7.	2.5-208	
						М	lodel	Secure Fire Center	wall Manag r for VMwar	ement e	M	Secu anager	re Firewal	l er for

O Principal e o Secundário mantêm a sincronização; isso é normal.

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		٩	☆
Cloud Services High Availability eStreamer	Host Input Client			Peer Manager
		Switc	ch Peer Roles 🛛 🐠 Break HA	II Pause Synchronization
Summary		System Status		
Status	Synchronization task is in progress	-,	Local	Remote
Synchronization	OK		(10.18.19.32)	(10.18.19.31)
Active System	10.18.19.31	Operating System	7.2.5	7.2.5
Standby System	10.18.19.32	Software Version	7.2.5-208	7.2.5-208
		Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Reserve alguns minutos para verificar se seus dispositivos estão sendo exibidos corretamente no primário e no secundário.

#### 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.