Configurar a alta disponibilidade do FTD em dispositivos Firepower

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Tarefa 1. Verificar condições
Tarefa 2. Configurar FTD HA
Condições
<u>Tarefa 3. Verificar HA do FTD e licença</u>
Tarefa 4. Alternar entre as funções de failover
Tarefa 5. Interromper o par de HA
Tarefa 6. Excluir um par HA
Tarefa 7. Suspender HA
Perguntas frequentes
Informações Relacionadas

Introdução

Este documento descreve como configurar e verificar o Firepower Threat Defense (FTD) High Availability (HA) (Failover Ativo/Standby) em dispositivos Firepower.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- 2x Cisco Firepower 9300
- 2x Cisco Firepower 4100 (7.2.8)
- Firepower Management Center (FMC) (7.2.8)

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.

Nobservação: em um dispositivo FPR9300 com FTD, você pode configurar somente HA entre chassis. As duas unidades em uma configuração de HA devem atender às condições mencionadas neste documento.

Tarefa 1. Verificar condições

Requisito da tarefa:

Verifique se ambos os dispositivos FTD atendem aos requisitos da nota e podem ser configurados como unidades HA.

Solução:

Etapa 1. Conecte-se ao IP de gerenciamento do FPR9300 e verifique o hardware do módulo.

Verifique o hardware do FPR9300-1.

<#root>

KSEC-FPR9K-1-A#

show server inventory

Server	Equipped PID	Equipped	VID Equipped Serial	(SN) Slot Status	Ackd Memory (MB) Ackd	Cores
1/1	FPR9K-SM-36	V01	FLM19216KK6	Equipped	262144	36
1/2	FPR9K-SM-36	V01	FLM19206H71	Equipped	262144	36
1/3	FPR9K-SM-36	V01	FLM19206H7T	Equipped	262144	36
KSEC-F	PR9K-1-A#					

Verifique o hardware do FPR9300-2.

<#root>

KSEC-FPR9K-2-A#

show server inventory

Server	Equipped PID	Equipped VID	Equipped Serial (SM	N) Slot Status	Ackd Memory (MB)	Ackd Cores
1/1	FPR9K-SM-36	V01	FLM19206H9T	Equipped	262144	36
1/2	FPR9K-SM-36	V01	FLM19216KAX	Equipped	262144	36
1/3	FPR9K-SM-36	V01	FLM19267A63	Equipped	262144	36
KSEC-FP	R9K-2-A#					

Etapa 2. Faça login no gerenciador de chassi do FPR9300-1 e navegue até os dispositivos

lógicos.

Verifique a versão do software, o número e o tipo de interfaces.

Tarefa 2. Configurar FTD HA

Requisito da tarefa:

Configure failover ativo/standby (HA) de acordo com este diagrama. Nesse caso, um par 41xx é usado.



Solução

Ambos os dispositivos do FTD já estão registrados no FMC, conforme mostrado na imagem.

FTD4100-5 Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	4S	1
FTD4100-6 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6:443 Escurity Module - 1	Base, Threat (2 more)	acp_simple	«Ç»	1:

Etapa 1. Para configurar o failover de FTD, navegue para Devices > Device Management e escolha Add High Availability como mostrado na imagem.

	Deploym	ent History
Q Search De	evice	Add 🔻
	Device	
	High A	vailability
Auto RollBack	Cluste	r
	Group	

Etapa 2. Insira o Par primário e o Par secundário e escolha Continuar como mostrado na imagem.

Add High Availability Pair Name:* FTD4100-HA Device Type: Firewall Threat Defense Primary Peer: FTD4100-5 Secondary Peer: FTD4100-6 Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		Lleancas
Name:* FTD4100-HA Device Type: Firewall Threat Defense Primary Peer: FTD4100-5 Secondary Peer: FTD4100-6 Total Defense High Availability pair will have primary configuration. Licenses from primary peer will be		0
FTD4100-HA Device Type: Firewall Threat Defense Primary Peer: FTD4100-5 Secondary Peer: FTD4100-6 ▼ On Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
Device Type: Firewall Threat Defense Primary Peer: FTD4100-5 Secondary Peer: FTD4100-6 Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be	nt (
Firewall Threat Defense • Primary Peer: • FTD4100-5 • Secondary Peer: • FTD4100-6 • O Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
Primary Peer: FTD4100-5 Secondary Peer: FTD4100-6 Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be	rt (
FTD4100-5 • Secondary Peer: • FTD4100-6 • Image: Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
Secondary Peer: FTD4100-6 Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
FTD4100-6 v Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be		
converted to their high availability versions and applied on both peers.		r will have primary y peer will be ersions and applied
Cancel Continue		Continue

Aviso: Selecione a unidade correta como a unidade primária. Todas as configurações na unidade primária selecionada são replicadas na unidade FTD secundária selecionada. Como resultado da replicação, a configuração atual na unidade secundária pode ser substituída.

Condições

Para criar uma HA entre os dois dispositivos do FTD, estas condições devem ser atendidas:

- O mesmo modelo
- Mesma versão aplica-se ao FXOS e ao FTD principal (primeiro número), secundário (segundo número) e manutenção (terceiro número) devem ser iguais.
- O mesmo número de interfaces
- O mesmo tipo de interfaces
- Ambos os dispositivos fazem parte do mesmo grupo/domínio no FMC.
- Ter uma configuração Network Time Protocol (NTP) idêntica.
- Ser plenamente instalado no CVP sem alterações não confirmadas.
- Estar no mesmo modo de firewall: roteado ou transparente.



Nota: Esta verificação deve ser feita nos dispositivos do FTD e na GUI do FMC, uma vez que houve casos em que os FTDs tinham o mesmo modo, mas o FMC não reflete isso.

Não tem DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configurado em nenhuma das interfaces.

Nome de host diferente [Fully Qualified Domain Name (FQDN)] para ambos os chassis.
 Para verificar o nome de host do chassi, navegue até FTD CLI e execute este comando:

```
<#root>
firepower#
show chassis-management-url
https://
KSEC-FPR9K-1.cisco.com
:443//
```

Observação: no FTD pós-6.3, use o comando show chassis detail.

<#root>

Firepower-module1#

show chassis detail

Chassis URL : https://FP4100-5:443//

Chassis IP : 10.62.148.187 Chassis IPv6 : :: Chassis Serial Number : JAD19500BAB Security Module : 1

Se os dois chassis tiverem o mesmo nome, altere o nome em um deles usando estes comandos:

<#root>

KSEC-FPR9K-1-A#

scope system

KSEC-FPR9K-1-A /system #

set name FPR9K-1new

Warning: System name modification changes FC zone name and redeploys them non-disruptively KSEC-FPR9K-1-A /system* #

commit-buffer

FPR9K-1-A /system #

exit

FPR9K-1new-A

Depois de alterar o nome do chassi, cancele o registro do FTD no FMC e registre-o novamente. Em seguida, continue a criação do par de HA.

Etapa 3. Configure a HA e indique as configurações de links.

No seu caso, o link de estado tem as mesmas configurações do link de alta disponibilidade.

Escolha Add e aguarde alguns minutos para que o par HA seja implantado, como mostrado na imagem.

ligh Availabi	lity Link	State Link		
Interface:*	Port-channel3 v	Interface:*	Same as LAN Failover Link	٣
ogical Name:*	FOVER	Logical Name:*	FOVER	
Primary IP:*	172.16.51.1	Primary IP:*	172.16.51.1	
Ì	Use IPv6 Address		Use IPv6 Address	
Secondary IP:*	172.16.51.2	Secondary IP:*	172.16.51.2	
Subnet Mask:*	255.255.255.0	Subnet Mask:*	255.255.255.0	
Psec Encryp	tion			
Key Generation:	Auto 🔻			
LAN failover l between peers.	ink is used to sync configuration, statefu Selected interface links and encryption s	ul failover link is used settings cannot be cl	t to sync application content hanged later.	

Etapa 4. Configurar as interfaces de dados (endereços IP primário e standby)

Na GUI do FMC, escolha o HA Edit como mostrado na imagem.

V FTD4120-HA High Availability							
FTD4100-5(Primary, Active) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	ŝ	1
FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	40	:

Etapa 5. Defina as configurações de interface:

Edit Physical Interface		0
General IPv4 IPv6 Par	th Monitoring Advanced	
Name:		
Inside		
Enabled		
Management Only		
Description:		
Mada.		
Mode:		
-		
Security Zone:		
•		
Interface ID:		
Ethernet1/4		
MTU:		
1500		
(64 - 9184)		
Priority:		
0	(0 - 65535)	
Propagate Security Group Tag:		
NVE Only:		
	Cancel	ж

Edit Physi	cal Inter	face						0
General	IPv4	IPv6	Path Monitoring	Advanced				
IP Type:								
IP Address:	IP		v					
192.168.7	5.10/24							
eg. 192.0.2.1/	255.255.25	5.128 or 19	2.0.2.1/25					
							Cancel	ОК

No caso de uma subinterface, é necessário primeiro habilitar a interface pai:

Edit Ether Channel Interface							
General	IPv4	IPv6	Path Monitoring	Advanced			
Name:	nent Only	,					
Description:							

Etapa 6. Navegue até High Availability e escolha o nome da interface Edit para adicionar os endereços IP de standby como mostrado na imagem.

Firewall Management Cer Devices / High Availability	overview	Analysis Policies	Devices Objects Integrati	on			Deploy Q 🔗 🔅	🛛 mzafeiro 🕶 🍟	SECURE
FTD4120-HA Cisco Firepower 4120 Threat Defense								Save	Cancel
Summary High Availability Devi	ce Routing Interfa	ces Inline Sets DI	HCP VTEP						
High Availability Configuration									
High Availability Link					State Link				
Interface			Port-channel3		Interface			Port-c	hannel3
Logical Name			FOVER		Logical Name				FOVER
Primary IP			172.16.51.1		Primary IP			172.	16.51.1
Secondary IP			172.16.51.2		Secondary IP			172.	16.51.2
Subnet Mask			255.255.255.0		Subnet Mask			255.25	5.255.0
IPsec Encryption			Disabled		Statistics				Q
Monitored Interfaces									
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	_
😭 Inside	192.168.75.10							•	1
diagnostic								•	1
Outside	192.168.76.10							•	1

Passo 7. Para a interface interna, conforme mostrado na imagem.

Edit Inside	0
Monitor this interface for failures	
Interface Name: Inside Active IP Address: 192.168.75.10 Mask: 24 Standby IP Address: 192.168.75.11	
	Cancel OK

Etapa 8. Faça o mesmo na interface externa.

Etapa 9. Verifique o resultado conforme mostrado na imagem.

Monitored Interfaces							
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
🔯 Inside	192.168.75.10	192.168.75.11				•	/
diagnostic						•	/
Outside	192.168.76.10	192.168.76.11				•	/

Etapa 10. Fique na guia Alta disponibilidade e configure endereços MAC virtuais conforme mostrado na imagem.

Interface MAC Addresses			+
Physical Interface Active Mac Address Standby Mac Address			
No records to display			

Etapa 11. Para a Interface interna é conforme mostrado na imagem.

Add Interface Mac Address
Physical Interface:*
Ethernet1/4
Active Interface Mac Address:*
aaaa.bbbb.1111
Standby Interface Mac Address:*
aaaa.bbbb.2222
Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab
Cancel OK

Etapa 12. Faça o mesmo na interface externa.

Etapa 13. Verifique o resultado conforme mostrado na imagem.

Interface MAC Addresses			+
Physical Interface	Active Mac Address	Standby Mac Address	
Ethernet1/4	aaaa.bbbb.1111	aaaa.bbbb.2222	/1
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	/1

Etapa 14. Depois de configurar as alterações, escolha Salvar e Implantar.

Tarefa 3. Verificar HA do FTD e licença

Requisito da tarefa:

Verifique as configurações de HA do FTD e licenças ativadas na GUI do FMC e na CLI do FTD.

Solução:

Etapa 1. Navegue até Resumo e verifique as configurações de HA e licenças ativadas, conforme mostrado na imagem.

Firewall Manag Devices / High Availa	ement Center Overview Analysis	Policies Devices Objects	Integration		Deploy Q	e	° 0
FTD4120-HA Cisco Firepower 4120 Three Summary High Avail	t Defense ability Device Routing Interfaces Inl	ne Sets DHCP VTEP					
	General		1±+	License			1
	Name:	FTD	4120-HA	Base:		[Yes
	Transfer Packets:		Yes	Export-Controlled Features:			No
	Status:		0	Malware:			Yes
	Primary Peer:	FTD4100-	5(Active)	Threat:			Yes
	Secondary Peer:	FTD4100-6	(Standby)	URL Filtering:			Yes
	Failover History:		Q	AnyConnect Apex:			No
				AnyConnect Plus:			No
				AnyConnect VPN Only:			No

Etapa 2. Na CLI FTD CLISH, execute o comando 'show high-availability config' ou 'show failover':

<#root>

>

```
show high-availability config
```

Failover On Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 2 of 1291 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(4)210, Mate 9.18(4)210 Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG

```
This host: Primary - Active
                Active time: 1999 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.10): Link Down (Shutdown)
                  Interface Outside (192.168.76.10): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Standby Ready
                Active time: 1466 (sec)
                slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface Inside (192.168.75.11): Link Down (Shutdown)
                  Interface Outside (192.168.76.11): Normal (Not-Monitored)
                slot 1: snort rev (1.0) status (up)
                slot 2: diskstatus rev (1.0) status (up)
Stateful Failover Logical Update Statistics
<output omitted>
```

Etapa 3. Faça o mesmo no dispositivo secundário.

Last Failover at: 08:46:30 UTC Jul 18 2024

Etapa 4. Execute o comando show failover state na CLI do LINA:

<#root>

firepower#

show failover state

This host -	State Primary	Last Failure Reason	Date/Time
Other host -	Active	None	
other host	Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016
====Configurat Sync Done ====Communicat Mac set	ion State=== ion State===		
firepower#			

Etapa 5. Verifique a configuração na unidade primária (CLI do LINA):

show running-config failover

>

```
failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2
>
show running-config interface
I
interface Port-channel2
no nameif
no security-level
no ip address
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
I
interface Port-channel3
description LAN/STATE Failover Interface
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
interface Ethernet1/4
shutdown
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
>
```

Tarefa 4. Alternar entre as funções de failover

Requisito da tarefa:

No FMC, alterne as funções de failover de primária/ativa, secundária/standby para primária/standby, secundária/ativa

Solução:

Etapa 1. Selecione o ícone conforme mostrado na imagem.

FTD4120-HA High Availability							Switch Active Peer
FTD4100-5(Primary, Active) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	C>	Force refresh node status Delete Revert Upgrade
FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	III Security Module - 1	Base, Threat (2 more)	acp_simple	Q\$	Health Monitor Troubleshoot Files

Etapa 2. Confirme a ação.

Você pode usar a saída do comando show failover history:

No novo Ative		
> show failover history		
Do Estado para o Motivo do Estado		
09:27:11 UTC Jul 18 2024 Pronto para Espera Apenas Ativo Outra unidade quer me Ativo config)	(Definido pelo comando	
09:27:11 UTC Jul 18 2024 Apenas Ativo Dreno Ativo Outra unidade quer-me Ativo config)	(Definido pelo comando	> show ===== Do Est
09:27:11 UTC Jul 18 2024 Dreno Ativo Aplicação Ativa Config Outra unidade quer-me Ativo config)	(Definido pelo comando	09:27:1 Pronto
09:27:11 UTC Jul 18 2024 Aplicando Ativo Config. Ativo Config. Aplicado Outra unidade quer me config)	Ativo (Definido pelo comando	
09:27:11 UTC Jul 18 2024 Config. Ativa Aplicada Ativa Outra unidade quer me Ativo config)	(Definido pelo comando	

Etapa 4. Após a verificação, ative a unidade primária novamente.

Tarefa 5. Interromper o par de HA

Requisito da tarefa:

No FMC, interrompa o par de failover.

Solução:

Etapa 1. Selecione o ícone conforme mostrado na imagem.

/ E
Switch Active Peer
Break
Force refresh node status
Delete
 Revert Upgrade
Health Monitor
Troubleshoot Files

Etapa 2. Verifique a notificação conforme mostrado na imagem.



Etapa 3. Observe a mensagem conforme mostrado na imagem.

Deployments Upgrades () Health () Tasks	Show Notifications
20+ total 0 waiting 0 running 0 retrying 20+ success 1 failure Q Filter	
Policy Deployment Policy Deployment to FTD4100-5. Applied successfully	47s ×
Policy Pre-Deployment Pre-deploy Device Configuration for FTD4100-5 success	<u>3s</u> ×
 Policy Pre-Deployment Pre-deploy Global Configuration Generation success 	<u>4s</u> ×
High Availability HA pair has been broken successfully and all policies have been retained on active peer FTD4100-6. St peer FTD4100-5 policies are being deleted by an auto triggered deployment. Please allow this deploym complete on FTD4100-5 before configuring its policies.	andby $\frac{1m 59s}{59s} \times$
Remove completed tasks	

Etapa 4. Verifique o resultado da GUI do FMC ou da CLI

show running-config na unidade primária antes e depois da interrupção da HA:

Unidade principal/em espera antes da quebra de HA	Unidade primária após a quebra de HA
> show running-config : Salvo :	> INFO: esta unidade está atualmente em estado de espera. Ao desabilitar o failover, essa unidade permanecerá no estado de espera.
: Numero de serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos)	> show running-config : Salvo :
NGFW versão 7.2.8 ! hostname firepower	: Número de série: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos)
strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6	: NGFW versão 7.2.8 !
nomes no mac-address auto !	habilitar senha ***** criptografada strong-encryption-disable service-module 0 keepalive-timeout 4
interface Port-channel2 no nameif manual cts propagate sot preserve-untag	service-module 0 keepalive-counter 6 nomes no mac-address auto
policy static sgt disabled trusted sem nível de segurança no ip address	! interface Port-channel2 fechamento no nameif
interface Port-channel2.202 vlan 202 nameif Externo	sem nível de segurança no ip address !
manual cts propagate sgt preserve-untag policy static sgt disabled trusted nível de segurança 0	fechamento no nameif sem nível de segurança
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port channel?	no ip address ! interface Ethernet1/1 somente gerenciamento
description LAN/STATE Failover Interface ! interface Ethernet1/1	fechamento no nameif sem nível de segurança
somente gerenciamento	no ip address

diagnóstico de nameif	!
manual cts	interface Ethernet1/4
propagate sgt preserve-untag	techamento
policy static sgt disabled trusted	no nameif
nível de segurança 0	sem nível de segurança
no ip address	no ip address
interface Ethernet1/4	ftp mode passive
nameif Interno	ngips conn-match vlan-id
manual cts	object-group-search access-control
propagate sgt preserve-untag	access-group CSM_FW_ACL_ global
policy static sgt disabled trusted	access-list CSM_FW_ACL_ remark rule-id
nível de segurança 0	9998: PREFILTER POLICY: Default Tunnel and
ip address 192.168.75.10 255.255.255.0 standby	Priority Policy
192.168.75.11	access-list CSM_FW_ACL_ remark rule-id
!	9998: RULE: DEFAULT TUNNEL ACTION
ftp mode passive	RULE
ngips conn-match vlan-id	access-list CSM_FW_ACL_ advanced permit
object-group-search access-control	ipinip any any rule-id 9998
access-group CSM_FW_ACL_ global	access-list CSM_FW_ACL_ advanced permit
access-list CSM_FW_ACL_ remark rule-id 9998:	udp any eq 3544 any range 1025 65535 rule-id
PREFILTER POLICY: Default Tunnel and Priority	9998
Policy	access-list CSM_FW_ACL_ advanced permit
access-list CSM_FW_ACL_ remark rule-id 9998:	udp any range 1025 65535 any eq 3544 rule-id
RULE: DEFAULT TUNNEL ACTION RULE	9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit 41
ipinip any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp	access-list CSM_FW_ACL_ advanced permit
any eq 3544 any range 1025 65535 rule-id 9998	gre any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp	access-list CSM_FW_ACL_ remark rule-id
any range 1025 65535 any eq 3544 rule-id 9998	268439552: ACCESS POLICY: acp_simple -
access-list CSM_FW_ACL_ advanced permit 41	Obrigatório
any any rule-id 9998	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ advanced permit gre	268439552: L7 RULE: rule1
any any rule-id 9998	access-list CSM_FW_ACL_ advanced permit ip
access-list CSM_FW_ACL_ remark rule-id	any any rule-id 268439552
268434433: ACCESS POLICY: acp_simple -	!
Default	tcp-map UM_STATIC_TCP_MAP
access-list CSM_FW_ACL_ remark rule-id	tcp-options range 6 7 allow
268434433: L4 RULE: DEFAULT ACTION RULE	tcp-options range 9 18 allow
access-list CSM_FW_ACL_ advanced permit ip	tcp-options range 20 255 allow (o intervalo de
any any rule-id 268434433	opções tcp 20 255 permite)
!	permissão de flag urgente
tcp-map UM_STATIC_TCP_MAP	!
tcp-options range 6 7 allow	sem pager
tcp-options range 9 18 allow	sem mensagem de log 106015

tcp-options range 20 255 allow (o intervalo de	sem mensagem de log 313001
opções tcp 20 255 permite)	sem mensagem de log 313008
permissão de flag urgente	sem mensagem de log 106023
!	sem mensagem de log 710003
sem pager	sem mensagem de log 106100
sem mensagem de log 106015	sem mensagem de log 302015
sem mensagem de log 313001	sem mensagem de log 302014
sem mensagem de log 313008	sem mensagem de log 302013
sem mensagem de log 106023	sem mensagem de log 302018
sem mensagem de log 710003	sem mensagem de log 302017
sem mensagem de log 106100	sem mensagem de log 302016
sem mensagem de log 302015	sem mensagem de log 302021
sem mensagem de log 302014	sem mensagem de log 302020
sem mensagem de log 302013	no failover
sem mensagem de log 302018	<saída omitida=""></saída>
sem mensagem de log 302017	
sem mensagem de log 302016	
sem mensagem de log 302021	
sem mensagem de log 302020	
mtu Outside 1500	
mtu diagnostic 1500	
mtu Inside 1500	
failover	
failover lan unit primary	
failover lan interface FOVER Port-channel3	
failover replication http	
failover mac address Ethernet1/4 aaaa.bbb.1111	
aaaa.bbbb.2222	
failover mac address Port-channel2.202	
aaaa.bbb.3333 aaaa.bbb.4444	
failover link FOVER Port-channel3	
failover interface ip FOVER 172.16.51.1	
255.255.255.0 standby 172.16.51.2	
<saida omitida=""></saida>	
Unidade secundaria/ativa antes da quebra de	Unidade secundária após a quebra de HA
HA	
> show rupping config	
- Salvo	> show running-config
:	
: Número de série: FLM2108V9YG	
: Hardware: FPR4K-SM-24, 73850 MB de RAM.	: Número de série: FLM2108V9YG
. , , , , , , , , , , , , , , , , , , ,	

CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos) :	: Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos)
NGEW versão 7.2.8	
	INGEW versão 7.2.8
' hostname firenower	
habilitar senha **** crintografada	i bostname firenower
strong-encryption-disable	habilitar senha **** crintografada
strong-encryption-disable	strong-encryption-disable
service-module 0 keepalive-timeout 4	sonvice module 0 keepalive timeout 4
	service-module 0 keepalive-timeout 4
no mac-address auto	nomes
	no mae addross auto
!	
interface Port-channel2	!
no nameif	interface Port-channel2
sem nível de seguranca	no nameif
no ip address	sem nível de seguranca
!	no ip address
interface Port-channel2.202	!
vlan 202	interface Port-channel2.202
nameif Externo	vlan 202
manual cts	nameif Externo
propagate sgt preserve-untag	manual cts
policy static sgt disabled trusted	propagate sgt preserve-untag
nível de segurança 0	policy static sgt disabled trusted
ip address 192.168.76.10 255.255.255.0	nível de segurança 0
standby 192.168.76.11	ip address 192.168.76.10 255.255.255.0
!	standby 192.168.76.11
interface Port-channel3	<u> </u>
description LAN/STATE Failover Interface	interface Port-channel3
!	no nameif
interface Ethernet1/1	sem nível de segurança
somente gerenciamento	no ip address
diagnóstico de nameif	!
nível de segurança 0	interface Ethernet1/1
no ip address	somente gerenciamento
!	diagnóstico de nameif
interface Ethernet1/4	nível de segurança 0
nameif Interno	no ip address
nível de segurança 0	!
ip address 192.168.75.10 255.255.255.0	interface Ethernet1/4
standby 192.168.75.11	nameif Interno
İ	nível de segurança 0
ftp mode passive	ip address 192.168.75.10 255.255.255.0
ngips conn-match vlan-id	standby 192.168.75.11

object-group-search access-control	!
access-group CSM_FW_ACL_ global	ftp mode passive
access-list CSM_FW_ACL_ remark rule-id 9998:	ngips conn-match vlan-id
PREFILTER POLICY: Default Tunnel and	object-group-search access-control
Priority Policy	access-group CSM FW ACL global
access-list CSM FW ACL remark rule-id 9998:	access-list CSM FW ACL remark rule-id 9998:
RULE: DEFAULT TUNNEL ACTION RULE	PREFILTER POLICY: Default Tunnel and
access-list CSM FW ACL advanced permit	Priority Policy
lipinip any any rule-id 9998	access-list CSM FW ACL remark rule-id 9998:
access-list CSM FW ACL advanced permit	RULE: DEFAULT TUNNEL ACTION RULE
udp any eg 3544 any range 1025 65535 rule-id	access-list CSM FW ACL advanced permit
9998	lipinip any any rule-id 9998
access-list CSM_EW_ACL_advanced permit	access-list CSM_FW_ACL_advanced permit
udp any range 1025 65535 any eq 3544 rule-id	udp any eg 3544 any range 1025 65535 rule-id
9998	9998
access-list CSM_EW_ACL_advanced permit 41	access-list CSM_EW_ACL_advanced permit
any any rule-id 9998	udp any range $1025\ 65535$ any eq 3544 rule-id
access-list CSM_EW_ACL_advanced permit gre	9998
any any rule-id 9998	access-list CSM_EW_ACL_advanced permit 41
access-list CSM_EW_ACIremark rule-id	any any rule-id 9998
268439552 ACCESS POLICY acp simple -	access-list CSM_EW_ACL_advanced permit are
	any any rule-id 9998
access-list CSM_EW_ACIremark rule-id	access-list CSM_EW_ACLremark rule-id
268439552° I 7 RUI E: rule1	268439552: ACCESS POLICY: acp. simple -
access-list CSM_EW_ACL_advanced permit in	
any any rule-id 268439552	access-list CSM_EW_ACLremark rule-id
	268439552 [·] L 7 RULE [·] rule1
tcp-map UM_STATIC_TCP_MAP	access-list CSM_EW_ACL_advanced permit ip
tcp-options range 6 7 allow	any any rule-id 268439552
tcp-options range 9 18 allow	
tcp-options range 20 255 allow (o intervalo de	tcp-map UM_STATIC_TCP_MAP
onções top 20 255 permite)	tcp-options range 6.7 allow
permissão de flag urgente	tcp-options range 9 18 allow
	tcp-options range 20 255 allow (o intervalo de
sem pager	oncões ton 20 255 permite)
sem mensagem de log 106015	permissão de flag urgente
sem mensagem de log 313001	
sem mensagem de log 313008	sem pager
sem mensagem de log 106023	sem mensagem de log 106015
sem mensagem de log 7100020	sem mensagem de log 313001
sem mensagem de log 106000	sem mensagem de log 313008
sem mensagem de log 302015	sem mensagem de log 106023
sem mensagem de log 302010	sem mensagem de log 7100020
sem mensagem de log 302014	sem mensagem de log 106100
sem mensagem de log 302018	sem mensagem de log 302015
sem mensagem de log 302010	sem mensagem de log 302013

sem mensagem de log 302016	sem mensagem de log 302013
sem mensagem de log 302021	sem mensagem de log 302018
sem mensagem de log 302020	sem mensagem de log 302017
mtu Outside 1500	sem mensagem de log 302016
mtu diagnostic 1500	sem mensagem de log 302021
mtu Inside 1500	sem mensagem de log 302020
failover	mtu Outside 1500
failover lan unit secondary	mtu diagnostic 1500
failover lan interface FOVER Port-channel3	mtu Inside 1500
failover replication http	no failover
failover link FOVER Port-channel3	no monitor-interface Outside
failover interface ip FOVER 172.16.51.1	no monitor-interface service-module
255.255.255.0 standby 172.16.51.2	
	<saída omitida=""></saída>
<saída omitida=""></saída>	

Os principais pontos a serem observados na interrupção da HA:

Unidade Principal/Standby	Unidade Secundária/Ativa
 Todas as configurações de failover foram removidas Toda a configuração IP é removida 	 Todas as configurações de failover foram removidas Os IPs em espera permanecem, mas são removidos na próxima implantação

Etapa 5. Depois de concluir essa tarefa, recrie o par de HA.

Tarefa 6. Excluir um par HA

Esta tarefa é baseada em uma configuração de HA em 41xx usando o software 7.2.8. Neste caso, inicialmente os dispositivos estavam nestes estados:

- Principal/Em espera
- Secundário/Ativo

Requisito da tarefa:

No FMC, exclua o par de failover.

Solução:

Etapa 1. Escolha o ícone conforme mostrado na imagem:

• •	FTD4120-HA High Availability							Switch Active Peer
	FTD4100-5(Primary, Standby) Short 3 10.62,148,188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	«Ş	Force refresh node status Delete Revert Uppracte
	FTD4100-6(Secondary, Active) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Health Monitor Troubleshoot Files

Etapa 2. Verifique e confirme a notificação conforme mostrado na imagem:

Confirm Delete
Are you sure you want to delete the high availability, "FTD4120-HA"? Deleting the pair from the Firewall Management Center does not disable high availability at the device level. The devices will continue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: "configure high-availability disable"
No Yes

Etapa 3. Depois que você excluir a HA, o registro dos dois dispositivos será cancelado (removido) do FMC.

O resultado do show running-config na CLI do LINA, conforme mostrado na tabela aqui:

Unidade Principal (Standby)	Unidade Secundária (Ativa)
> show running-config	> show running-config
: Salvo	: Salvo
:	:
: Número de série: FLM1949C5RR	: Número de série: FLM2108V9YG
: Hardware: FPR4K-SM-24, 73853 MB de RAM,	: Hardware: FPR4K-SM-24, 73853 MB de RAM,
CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48	CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48
núcleos)	núcleos)
:	:
NGFW versão 7.2.8	NGFW versão 7.2.8
!	!
hostname Firepower-module1	hostname Firepower-module1
habilitar senha ***** criptografada	habilitar senha ***** criptografada
strong-encryption-disable	strong-encryption-disable
no asp inspect-dp ack-passthrough	no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4	service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6	service-module 0 keepalive-counter 6
nomes	nomes

no mac-address auto	no mac-address auto
! interface Port channel?	! interface Port channel?
sem nível de segurança	
no in address	no in address
interface Port-channel2 202	interface Port-channel2 202
vlan 202	vlan 202
nomese NET202	nomese NET202
manual cts	manual cts
propagate sgt preserve-untag	propagate sgt preserve-untag
policy static sgt disabled trusted	policy static sgt disabled trusted
nível de segurança 0	nível de segurança 0
ip address 172.16.202.1 255.255.255.0 standby	ip address 172.16.202.1 255.255.255.0 standby
172.16.202.2	172.16.202.2
!	!
interface Port-channel2.203	interface Port-channel2.203
vlan 203	vlan 203
nomese NET203	nomese NET203
manual cts	manual cts
propagate sgt preserve-untag	propagate sgt preserve-untag
policy static sgt disabled trusted	policy static sgt disabled trusted
nível de segurança 0	nível de segurança 0
ip address 172.16.203.1 255.255.255.0 standby	ip address 172.16.203.1 255.255.255.0 standby
172.16.203.2	172.16.203.2
! interface Dart channel?	! interface Dart shannel?
Interface Port-channels	Intenace Port-channels
: interface Ethernet1/1	: interface Ethernet1/1
somente gerenciamento	somente gerenciamento
diagnóstico de nameif	diagnóstico de nameif
manual cts	manual cts
propagate sgt preserve-untag	propagate sgt preserve-untag
policy static sgt disabled trusted	policy static sgt disabled trusted
nível de segurança 0	nível de segurança 0
no ip address	no ip address
!	!
interface Ethernet1/4	interface Ethernet1/4
nomese NET204	nomese NET204
manual cts	manual cts
propagate sgt preserve-untag	propagate sgt preserve-untag
policy static sgt disabled trusted	policy static sgt disabled trusted
nivel de segurança 0	nivel de segurança 0
1	

ip address 172.16.204.1 255.255.255.0 standby	ip address 172.16.204.1 255.255.255.0 standby
172.16.204.2	172.16.204.2
!	!
ftp mode passive	ftp mode passive
ngips conn-match vlan-id	ngips conn-match vlan-id
no object-group-search access-control	no object-group-search access-control
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:	access-list CSM_FW_ACL_ remark rule-id 9998:
PREFILTER POLICY: Default Tunnel and	PREFILTER POLICY: Default Tunnel and
Priority Policy	Priority Policy
access-list CSM_FW_ACL_ remark rule-id 9998:	access-list CSM_FW_ACL_ remark rule-id 9998:
RULE: DEFAULT TUNNEL ACTION RULE	RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998	ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id 9998	udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id	udp any range 1025 65535 any eq 3544 rule-id
9998	9998
access-list CSM_FW_ACL_ advanced permit 41	access-list CSM_FW_ACL_ advanced permit 41
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre	access-list CSM_FW_ACL_ advanced permit gre
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433: ACCESS POLICY: acp_simple -	268434433: ACCESS POLICY: acp_simple -
Default	Default
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433: L4 RULE: DEFAULT ACTION	268434433: L4 RULE: DEFAULT ACTION
RULE	RULE
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ advanced permit ip
any any rule-id 268434433	any any rule-id 268434433
!	!
tcp-map UM_STATIC_TCP_MAP	tcp-map UM_STATIC_TCP_MAP
tcp-options range 6 / allow	tcp-options range 6 / allow
tcp-options range 9 18 allow	tcp-options range 9 18 allow
tcp-options range 20 255 allow (o intervalo de	tcp-options range 20 255 allow (o intervalo de
opçoes tcp 20 255 permite)	opçoes tcp 20 255 permite)
tcp-options md5 clear	tcp-options md5 clear
permissao de flag urgente !	permissao de flag urgente !
sem pager	sem pager
sem mensagem de log 106015	sem mensagem de log 106015
sem mensagem de log 313001	sem mensagem de log 313001
sem mensagem de log 313008	sem mensagem de log 313008
sem mensagem de log 106023	sem mensagem de log 106023

sem mensagem de log 710003 sem mensagem de log 106100 sem mensagem de log 302015 sem mensagem de log 302014 sem mensagem de log 302013 sem mensagem de log 302018 sem mensagem de log 302017 sem mensagem de log 302016 sem mensagem de log 302021 sem mensagem de log 302020 MTU NET202 1500 MTU NET203 1500 mtu diagnostic 1500 MTU NET204 1500 failover failover lan unit primary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <saída omitida> > show ip Enderecos IP do sistema: Nome da interface Endereço IP Máscara de sub-rede Método Canal de porta 2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Canal de porta 2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.1 255.255.255.0 desativado Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Endereços IP atuais: Nome da interface Endereço IP Máscara de sub-rede Método Canal de porta 2.202 NET202 172.16.202.2 255.255.255.0 CONFIG Canal de porta 2.203 NET203 172.16.203.2

sem mensagem de log 710003 sem mensagem de log 106100 sem mensagem de log 302015 sem mensagem de log 302014 sem mensagem de log 302013 sem mensagem de log 302018 sem mensagem de log 302017 sem mensagem de log 302016 sem mensagem de log 302021 sem mensagem de log 302020 MTU NET202 1500 MTU NET203 1500 mtu diagnostic 1500 MTU NET204 1500 failover failover lan unit secondary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 monitor-interface NET202 monitor-interface NET203 icmp unreachable rate-limit 1 burst-size 1 <saída omitida> > show ip Endereços IP do sistema: Nome da interface Endereço IP Máscara de sub-rede Método Canal de porta 2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Canal de porta 2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Port-channel3 FOVER 172.16.51.1 255.255.255.0 desativado Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Endereços IP atuais: Nome da interface Endereço IP Máscara de sub-rede Método Canal de porta 2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Canal de porta 2.203 NET203 172.16.203.1

255.255.255.0 CONFIG	255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.2
255.255.255.0 desativado	255,255,255,0 unset
Ethernet1/4 NET204 172 16 204 2	Ethernet1/4 NET204 172 16 204 1
255 255 255 0 CONFIG	255 255 255 0 CONFIG
> show failover	> show failover
Failover Ativado	Failover Ativado
Unidade de failover primária	Unidade de failover Secundária
Interface de LAN de failover: FOVER Port-	Interface de LAN de failover: FOVER Port-
channel3 (ativo)	channel3 (ativo)
Tempo limite de reconexão 0:00:00	Tempo limite de reconexão 0:00:00
Frequência de Sondagem de Unidade 1	Frequência de Sondagem de Unidade 1
segundo, tempo de espera 15 segundos	segundo, tempo de espera 15 segundos
Frequência de pesquisa de interface de 5	Frequência de pesquisa de interface de 5
segundos, tempo de espera de 25 segundos	segundos, tempo de espera de 25 segundos
Política de interface 1	Política de interface 1
Interfaces Monitoradas 4 de um máximo de	Interfaces Monitoradas 4 de um máximo de
1291	1291
Intervalo de Notificação de Movimentação de	Intervalo de Notificação de Movimentação de
Endereço MAC não definido	Endereço MAC não definido
failover replication http	failover replication http
Versão: Nosso 9.18(4)210, Companheiro	Versão: Nosso 9.18(4)210, Companheiro
9.18(4)210	9.18(4)210
Número de série: FLM1949C5RR, Mate	Número de série: FLM2108V9YG, Mate
FLM2108V9YG	FLM1949C5RR
Último failover em: 13:56:37 UTC, 16 de julho	Último failover em: 13:42:35 UTC, 16 de julho
de 2024	de 2024
Este host: Principal - Pronto para Espera	Este host: Secundário - Ativo
Tempo ativo: 0 (seg)	Tempo ativo: 70312 (s)
slot 0: status UCSB-B200-M3-U hw/sw rev	slot 0: status UCSB-B200-M3-U hw/sw rev
(0.0/9.18(4)210) (sistema ativo)	(0.0/9.18(4)210) (sistema ativo)
Interface NET202 (172.16.202.2): Normal	Interface NET202 (172.16.202.1): Normal
(Monitorada)	(Monitorada)
Interface NET203 (172.16.203.2): Normal	Interface NET203 (172.16.203.1): normal
(Monitorada)	(monitorada)
Diagnóstico da interface (0.0.0.0): normal	Diagnóstico da interface (0.0.0.0): normal
(aguardando)	(aguardando)
Interface NET204 (172.16.204.2): Normal	Interface NET204 (172.16.204.1): normal
(Monitorada)	(monitorada)
slot 1: snort rev (1.0) status (up)	slot 1: snort rev (1.0) status (up)
slot 2: status do diskstatus rev (1.0) (up)	slot 2: status do diskstatus rev (1.0) (up)
Outro host: secundário - ativo	Outro host: Principal - Pronto para Standby
Tempo ativo: 70293 (s)	Tempo ativo: 0 (seg)
Interface NET202 (172.16.202.1): Normal	slot 0: status UCSB-B200-M3-U hw/sw rev
(Monitorada)	(0.0/9.18(4)210) (sistema ativo)

Interface NET203 (172.16.203.1): normal	Interface NET202 (172.16.202.2): Normal
(monitorada)	(Monitorada)
Diagnóstico da interface (0.0.0.0): normal	Interface NET203 (172.16.203.2): Normal
(aguardando)	(Monitorada)
Interface NET204 (172.16.204.1): normal	Diagnóstico da interface (0.0.0.0): normal
(monitorada)	(aguardando)
slot 1: snort rev (1.0) status (up)	Interface NET204 (172.16.204.2): Normal
slot 2: status do diskstatus rev (1.0) (up)	(Monitorada)
	slot 1: snort rev (1.0) status (up)
<saída omitida=""></saída>	slot 2: status do diskstatus rev (1.0) (up)
	<saida omitida=""></saida>

Etapa 4. O registro de ambos os dispositivos do FTD foi cancelado no FMC:

<#root>

> show managers

No managers configured.

Os principais pontos a serem observados para a opção Desativar HA no FMC:

Unidade primária	Unidade secundária
O dispositivo foi removido do FMC. Nenhuma configuração foi removida do	O dispositivo foi removido do FMC. Nenhuma configuração foi removida do
dispositivo do FTD.	dispositivo do FTD.

Cenário 1

Execute o comando 'configure high-availability disable' para remover a configuração de failover do dispositivo de FTD ativo:

<#root>

>

configure high-availability disable

?

Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear <cr>

```
<#root>
```

>

configure high-availability disable

High-availability will be disabled. Do you really want to continue? Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.

O resultado:

Unidade principal (ex-Standby)	Unidade secundária (ex-ativa)
 > INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > show failover Failover Off (pseudo-Standby) Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) 	 > show failover Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum
Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25	MAC Address Move Notification Interval not set
seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http	> show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0
> show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset	CONFIG Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG

Principal (ex-Standby)	Secundário (ex-Ativo)
> show running-config : Salvo	> show running-config : Salvo
: : Número de série: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos)	: : Número de série: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon série E5 de 2.200 MHz, 2 CPUs (48 núcleos)
NGFW versão 7.2.8 I	NGFW versão 7.2.8 I
hostname Firepower-module1 habilitar senha ***** criptografada strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 nomes no mac-address auto	hostname Firepower-module1 habilitar senha ***** criptografada strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 nomes no mac-address auto
1	
interface Port-channel2 fechamento no nameif sem nível de segurança	interface Port-channel2 no nameif sem nível de segurança no ip address
interface Port-channel3 description LAN/STATE Failover Interface	interface Port-channel2.202 vlan 202 nomese NET202 manual cts
interface Ethernet1/1 somente gerenciamento fechamento no nameif sem nível de segurança no in address	propagate sgt preserve-untag policy static sgt disabled trusted nível de segurança 0 ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2
Interface Ethernet1/4 fechamento no nameif sem nível de segurança no ip address	interface Port-channel2.203 vlan 203 nomese NET203 manual cts propagate sgt preserve-untag policy static sgt disabled trusted
ftp mode passive	ip address 172.16.203.1 255.255.255.0 standby

ngips conn-match vlan-id	172.16.203.2
no object-group-search access-control	!
access-group CSM_FW_ACL_ global	interface Port-channel3
access-list CSM_FW_ACL_ remark rule-id 9998:	no nameif
PREFILTER POLICY: Default Tunnel and	sem nível de segurança
Priority Policy	no ip address
access-list CSM_FW_ACL_ remark rule-id 9998:	!
RULE: DEFAULT TUNNEL ACTION RULE	interface Ethernet1/1
access-list CSM_FW_ACL_ advanced permit	somente gerenciamento
ipinip any any rule-id 9998	diagnóstico de nameif
access-list CSM_FW_ACL_ advanced permit	manual cts
udp any eq 3544 any range 1025 65535 rule-id	propagate sgt preserve-untag
9998	policy static sgt disabled trusted
access-list CSM_FW_ACL_ advanced permit	nível de segurança 0
udp any range 1025 65535 any eq 3544 rule-id	no ip address
9998	!
access-list CSM_FW_ACL_ advanced permit 41	interface Ethernet1/4
any any rule-id 9998	nomese NET204
access-list CSM_FW_ACL_ advanced permit gre	manual cts
any any rule-id 9998	propagate sgt preserve-untag
access-list CSM_FW_ACL_ remark rule-id	policy static sgt disabled trusted
268434433: ACCESS POLICY: acp_simple -	nível de segurança 0
Default	ip address 172.16.204.1 255.255.255.0 standby
access-list CSM_FW_ACL_ remark rule-id	172.16.204.2
268434433: L4 RULE: DEFAULT ACTION	!
RULE	ftp mode passive
access-list CSM_FW_ACL_ advanced permit ip	ngips conn-match vlan-id
any any rule-id 268434433	no object-group-search access-control
!	access-group CSM_FW_ACL_ global
tcp-map UM_STATIC_TCP_MAP	access-list CSM_FW_ACL_ remark rule-id 9998:
tcp-options range 6 7 allow	PREFILTER POLICY: Default Tunnel and
tcp-options range 9 18 allow	Priority Policy
tcp-options range 20 255 allow (o intervalo de	access-list CSM_FW_ACL_ remark rule-id 9998:
opções tcp 20 255 permite)	RULE: DEFAULT TUNNEL ACTION RULE
tcp-options md5 clear	access-list CSM_FW_ACL_ advanced permit
permissão de flag urgente	ipinip any any rule-id 9998
!	access-list CSM_FW_ACL_ advanced permit
sem pager	udp any eq 3544 any range 1025 65535 rule-id
sem mensagem de log 106015	9998
sem mensagem de log 313001	access-list CSM_FW_ACL_ advanced permit
sem mensagem de log 313008	udp any range 1025 65535 any eq 3544 rule-id
sem mensagem de log 106023	9998
sem mensagem de log 710003	access-list CSM_FW_ACL_ advanced permit 41
sem mensagem de log 106100	any any rule-id 9998
sem mensagem de log 302015	access-list CSM_FW_ACL_ advanced permit gre
sem mensagem de log 302014	any any rule-id 9998

sem mensagem de log 302013	access-list CSM_FW_ACL_ remark rule-id
sem mensagem de log 302018	268434433: ACCESS POLICY: acp_simple -
sem mensagem de log 302017	Default
sem mensagem de log 302016	access-list CSM_FW_ACL_ remark rule-id
sem mensagem de log 302021	268434433: L4 RULE: DEFAULT ACTION
sem mensagem de log 302020	RULE
no failover	access-list CSM_FW_ACL_ advanced permit ip
failover lan unit primary	any any rule-id 268434433
failover lan interface FOVER Port-channel3	!
failover replication http	tcp-map UM_STATIC_TCP_MAP
failover link FOVER Port-channel3	tcp-options range 6 7 allow
failover interface ip FOVER 172.16.51.1	tcp-options range 9 18 allow
255.255.255.0 standby 172.16.51.2	tcp-options range 20 255 allow (o intervalo de
no monitor-interface service-module	opções tcp 20 255 permite)
	tcp-options md5 clear
<saída omitida=""></saída>	permissão de flag urgente
	!
	sem pager
	sem mensagem de log 106015
	sem mensagem de log 313001
	sem mensagem de log 313008
	sem mensagem de log 106023
	sem mensagem de log 710003
	sem mensagem de log 106100
	sem mensagem de log 302015
	sem mensagem de log 302014
	sem mensagem de log 302013
	sem mensagem de log 302018
	sem mensagem de log 302017
	sem mensagem de log 302016
	sem mensagem de log 302021
	sem mensagem de log 302020
	MTU NET202 1500
	MTU NET203 1500
	mtu diagnostic 1500
	MTU NET204 1500
	no failover
	monitor-interface NET202
	monitor-interface NET203
	no monitor-interface service-module

Principais pontos a serem observados para Desabilitar HA da CLI de FTD ativa:

Unidade Ativa

 Configuração d 	le failover
removida	
	~ ~

- Os IPs em espera não são removidos
- As configurações de interface foram removidas.
- A configuração de failover não é removida, mas o failover é desabilitado (pseudo-Standby)

Neste ponto, você pode desativar o HA também na unidade de ex-Standby.

Cenário 2 (Não recomendado)

Aviso: este cenário leva a uma situação Ativo/Ativo, portanto, não é recomendável. Ele é mostrado apenas para conscientização.

Execute o comando 'configure high-availability disable' para remover a configuração de failover do dispositivo FTD de standby:

<#root>

>

configure high-availability disable

High-availability will be disabled. Do you really want to continue? Please enter 'YES' or 'NO':

YES

Successfully disabled high-availability.

O resultado:

Principal (ex-Standby)	Secundário (Ativo)
 > show failover Failover Desativado Unidade de failover Secundária Interface de LAN de failover: não configurada Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos Política de interface 1 	 > show failover Failover em <- O failover não está desabilitado Unidade de failover Secundária Interface de LAN de failover: FOVER Port- channel3 (ativo) Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos

Interfaces Monitoradas 4 de um máximo de	Política de interface 1
1291	Interfaces Monitoradas 4 de um máximo de
Intervalo de Notificação de Movimentação de	1291
Endereço MAC não definido	Intervalo de Notificação de Movimentação de
	Endereço MAC não definido
	failover replication http
> show ip	Versão: Nosso 9.18(4)210, Companheiro
Endereços IP do sistema:	9.18(4)210
Nome da interface Endereço IP Máscara de	Número de série: FLM2108V9YG. Mate
sub-rede Método	FLM1949C5RR
Port-channel2.202 NET202 172.16.202.1	Último failover em: 12:44:06 UTC 17 de julho
255.255.255.0 manual <- O dispositivo usa os	de 2024
mesmos IPs que o ex-Ative!	Este host: Secundário - Ativo
Port-channel2.203 NET203 172.16.203.1	Tempo ativo: 632 (sea)
255.255.255.0 manual	clot 0: status LICSB B200 M2 LI bw/sw rov
Ethernet1/4 NET204 172.16.204.1	SIDE U. Status UCSD-D200-MIS-U Hw/SW TeV $(0, 0/0, 18(4))$
255 255 255 0 manual	(0.0/9, 10(4)210) (sisterna alivo)
Enderecos IP atuais:	
Nome da interface Endereco IP Máscara de	
sub-rede Método	Interface NE1204 (172.16.204.1): normal
Port-channel2 202 NET202 172 16 202 1	
255 255 255 0 manual	Interface NE1203 (1/2.16.203.1): normal
Dort oboppol2 202 NET202 172 16 202 1	(monitorada)
255 255 255 0 manual	Interface NET202 (172.16.202.1): Normal
Ethornot1/4 NET204 172 16 204 1	(Monitorada)
Ethemet 1/4 NET 204 172. 10.204. 1	slot 1: snort rev (1.0) status (up)
255.255.255.0 manual	slot 2: status do diskstatus rev (1.0) (up)
	Outro host: Principal - Desabilitado
	Tempo ativo: 932 (seg)
	slot 0: status UCSB-B200-M3-U hw/sw rev
	(0.0/9.18(4)210) (sistema ativo)
	Diagnóstico de interface (0.0.0.0): desconhecido
	(aguardando)
	Interface NET204 (172.16.204.2): Desconhecida
	(Monitorada)
	Interface NET203 (172.16.203.2): Desconhecida
	(Monitorada)
	Interface NET202 (172.16.202.2): Desconhecida
	(Monitorada)
	slot 1: snort rev (1.0) status (up)
	slot 2: status do diskstatus rev (1.0) (up)
	> show ip
	Endereços IP do sistema:
	Nome da interface Endereço IP Máscara de
	sub-rede Método
	Port-channel2.202 NET202 172.16.202.1

255.255.255.0 manual <- O dispositivo usa os
mesmos IPs que o ex-Standby!
Port-channel2.203 NET203 172.16.203.1
255.255.255.0 manual
Port-channel3 FOVER 172.16.51.1
255.255.255.0 desativado
Ethernet1/4 NET204 172.16.204.1
255.255.255.0 manual
Endereços IP atuais:
Nome da interface Endereço IP Máscara de
sub-rede Método
Port-channel2.202 NET202 172.16.202.1
255.255.255.0 manual
Port-channel2.203 NET203 172.16.203.1
255.255.255.0 manual
Port-channel3 FOVER 172.16.51.2
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1
255.255.255.0 manual

Principais pontos a serem observados para Desabilitar HA da CLI de FTD ativa:

Unidade Ativa	Unidade em Espera
 A configuração de failover não é removida e permanece habilitada O dispositivo usa os mesmos IPs que a unidade de ex- standby 	 Configuração de failover removida O dispositivo usa os mesmos IPs que a unidade Ativa

Cenário 3

Execute o comando 'configure high-availability disable clear-interfaces' para remover a configuração de failover do dispositivo de FTD ativo:

<#root>

>

configure high-availability disable clear-interfaces

High-availability will be disabled. Do you really want to continue? Please enter 'YES' or 'NO':

>

O resultado:

Principal (ex-Standby)	Secundário (ex-Ativo)
 > show failover Failover Desativado (pseudo-Standby) Unidade de failover primária Interface de LAN de failover: FOVER Port- channel3 (ativo) Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos Política de interface 1 Interfaces Monitoradas 0 de no máximo 1291 Intervalo de Notificação de Movimentação de Endereço MAC não definido failover replication http 	 > show failover Failover Desativado Unidade de failover Secundária Interface de LAN de failover: não configurada Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos Política de interface 1 Interfaces Monitoradas 0 de no máximo 1291 Intervalo de Notificação de Movimentação de Endereço MAC não definido
 > show ip Endereços IP do sistema: Nome da interface Endereço IP Máscara de sub-rede Método Port-channel3 FOVER 172.16.51.1 255.255.255.0 desativado Endereços IP atuais: Nome da interface Endereço IP Máscara de sub-rede Método Port-channel3 FOVER 172.16.51.1 255.255.255.0 desativado > 	> show ip Endereços IP do sistema: Nome da interface Endereço IP Máscara de sub-rede Método Endereços IP atuais: Nome da interface Endereço IP Máscara de sub-rede Método >

Pontos principais a serem observados para Desabilitar HA junto com 'clear-interfaces' da CLI de FTD Ativo:

Unidade Ativa	Unidade em Espera

 Configuração de failover removida Os IPs são removidos 	 A configuração de failover não é removida, mas o failover é desabilitado (pseudo-Standby) Os IPs são removidos

Cenário 4

Execute o comando 'configure high-availability disable clear-interfaces' para remover a configuração de failover do dispositivo FTD de standby:

<#root>

>

configure high-availability disable clear-interfaces

High-availability will be disabled. Do you really want to continue? Please enter 'YES' or 'NO':

YES

Successfully disabled high-availability.

>

O resultado:

Principal (ex-Standby)	Secundário (Ativo)
 > show failover Failover Desativado Unidade de failover Secundária Interface de LAN de failover: não configurada Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos Política de interface 1 Interfaces Monitoradas 0 de no máximo 1291 Intervalo de Notificação de Movimentação de Endereço MAC não definido 	 > show failover Failover Ativado Unidade de failover Secundária Interface de LAN de failover: FOVER Port- channel3 (ativo) Tempo limite de reconexão 0:00:00 Frequência de Sondagem de Unidade 1 segundo, tempo de espera 15 segundos Frequência de pesquisa de interface de 5 segundos, tempo de espera de 25 segundos Política de interface 1 Interfaces Monitoradas 4 de um máximo de 1291 Intervalo de Notificação de Movimentação de Endereço MAC não definido

> show ip Endereços IP do sistema:	failover replication http Versão: Nosso 9.18(4)210, Companheiro
Nome da interface Endereço IP Máscara de	9.18(4)210
sub-rede Método	Número de série: FLM2108V9YG, Mate
Endereços IP atuais:	FLM1949C5RR
Nome da Interface Endereço IP Mascara de	de 2024
>	Este host: Secundário - Ativo
	Tempo ativo: 1194 (seg)
	slot 0: status UCSB-B200-M3-U hw/sw rev
	(0.0/9.18(4)210) (sistema ativo)
	Diagnóstico da interface (0.0.0.0): normal
	(aguardando)
	Interface NET204 (172.16.204.1): normal
	(monitorada)
	Interface NET202 (172.16.202.1): Normal
	(Monitorada)
	Interface NET203 (172.16.203.1): normal
	(monitorada)
	slot 1. short rev (1.0) status (up) slot 2: status do diskstatus rev (1.0) (up)
	Outro host: Principal - Desabilitado
	Tempo ativo: 846 (seg)
	slot 0: status UCSB-B200-M3-U hw/sw rev
	(0.0/9.18(4)210) (sistema ativo)
	Diagnóstico de interface (0.0.0.0): desconhecido
	(aguardando)
	Interface NET204 (172.16.204.2): Desconhecida
	(Monitorada)
	Interface NET202 (172.16.202.2): Desconhecida
	(Monitorada)
	Interface NET203 (172.16.203.2): Desconhecida
	(Monitorada)
	slot 2: status do diskstatus rev (1.0) (up)
	> show ip
	Endereços IP do sistema:
	Nome da interface Endereço IP Máscara de
	sub-rede Método
	Port-channel2.202 NET202 172.16.202.1
	255.255.255.0 manual
	255 255 255 0 mapual
	Port-channel3 FOVER 172 16 51 1
	255 255 255 0 desativado

Eth	nernet1/4 NET204 172.16.204.1
255	5.255.255.0 manual
End	dereços IP atuais:
No	me da interface Endereço IP Máscara de
sub	o-rede Método
Pol	rt-channel2.202 NET202 172.16.202.1
255	5.255.255.0 manual
Pol	rt-channel2.203 NET203 172.16.203.1
255	5.255.255.0 manual
Pol	rt-channel3 FOVER 172.16.51.2
255	5.255.255.0 unset
Eth	nernet1/4 NET204 172.16.204.1
255	5.255.255.0 manual

Pontos principais a serem observados para Desabilitar HA junto com 'clear-interfaces' da CLI de FTD Ativo:

Unidade Ativa	Unidade em Espera
 Configuração de failover não	 Configuração de failover
removida Os IPs não são removidos	removida Os IPs são removidos

Etapa 6. Depois de concluir a tarefa, registre os dispositivos no FMC e ative o par de HA.

Tarefa 7. Suspender HA

Requisito da tarefa:

Suspender a HA na CLI CLISH do FTD

Solução:

Etapa 1. No FTD primário, execute o comando e confirme (digite SIM).

<#root>

> configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability. Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.

Etapa 2. Verifique as alterações na unidade primária:

<#root>

>

show high-availability config

Failover Off

Failover unit Primary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set failover replication http

Etapa 3. O resultado na unidade secundária:

<#root>

>

show high-availability config
Failover Off (pseudo-Standby)

Failover unit Secondary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set failover replication http

Etapa 4. Retome a HA na unidade primária:

<#root>

>

configure high-availability resume

Successfully resumed high-availablity.

> .

End Configuration Replication to mate

>

<#root>

>

show high-availability config

Failover On

Failover unit Primary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1041 maximum MAC Address Move Notification Interval not set failover replication http

Etapa 5. O resultado na unidade secundária após a retomada da HA:

<#root>

> ..

Detected an Active mate

Beginning configuration replication from mate.

WARNING: Failover is enabled but standby IP address is not configured for this interface. WARNING: Failover is enabled but standby IP address is not configured for this interface. End configuration replication from mate.

>

<#root>

>

show high-availability config

Failover On

Failover unit Secondary Failover LAN Interface: fover_link Ethernet1/4 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1

Perguntas frequentes

Quando a configuração é replicada, ela é salva imediatamente (linha por linha) ou no final da replicação?

Ao final da replicação. A comprovação está no final da saída do comando debug fover sync, que mostra a replicação de configuração/comando:

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
. . .
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:
write memory
                   <--
```

O que acontece se uma unidade estiver em um estado pseudo-Standby (failover desabilitado) e você recarregá-la enquanto a outra unidade estiver com o failover habilitado e Ativo? Você acaba em um cenário Ativo/Ativo (embora tecnicamente seja um Ativo/Failover-desativado). Especificamente, quando a unidade se torna ATIVA, o failover é desativado, mas a unidade usa os mesmos IPs que a unidade ativa. Então, de fato, você tem:

- Unidade-1: Ativa
- Unidade 2: failover desativado. A unidade usa os mesmos IPs de dados que a Unidade-1, mas endereços MAC diferentes.

O que acontece com a configuração de failover se você desabilitar manualmente o failover

(configurar suspensão de alta disponibilidade) e recarregar o dispositivo? Quando você desabilita o failover, ele não é uma alteração permanente (não salva na configuração de inicialização, a menos que você decida fazer isso explicitamente). Você pode reinicializar/recarregar a unidade de duas maneiras diferentes e, com a segunda, você deve ter cuidado:

Caso 1. Reiniciar no CLISH

A reinicialização no CLISH não solicita confirmação. Assim, a alteração de configuração não é salva em startup-config:

<#root>

>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability. Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to

YES

Successfully suspended high-availability.

A configuração atual tem o failover desabilitado. Nesse caso, a unidade estava em Standby e entrou no estado pseudo-Standby como esperado para evitar um cenário Ativo/Ativo:

<#root>
firepower#
show failover | include Failover
Failover Off (
pseudo-Standby
)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)

A configuração de inicialização ainda tem o failover habilitado:

<#rOOt>
firepower#
show startup | include failover
failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****

Reinicialize o dispositivo no CLISH (comando reboot):

<#root>

>

reboot

```
This command will reboot the system. Continue? Please enter 'YES' or 'NO':
```

YES

```
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

Quando a unidade está em ATIVA e o failover está ativado, o dispositivo entra na fase de negociação de failover e tenta detectar o par remoto:

<#root>

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

Detected an Active mate

Caso 2. Reinicialização na CLI do LINA

A reinicialização no LINA (comando reload) solicita a confirmação. Assim, caso você selecione Y (Yes), a alteração de configuração é salva em startup-config:

<#root>

firepower#

reload

System config has been modified. Save? [Y]es/[N]o:

Y <-- Be careful. This disables the failover in the startup-config

Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs Proceed with reload? [confirm] firepower#

show startup | include failover

no failover

failover lan unit secondary failover lan interface FOVER Ethernet1/1 failover replication http failover link FOVER Ethernet1/1 failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2 failover ipsec pre-shared-key *****

Depois que a unidade estiver ATIVA, o failover será desativado:

<#root>

firepower# show failover | include Fail Failover Off

Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/1 (up)



No Servação: para evitar esse cenário, certifique-se de não salvar as alterações na configuração de inicialização quando for solicitado.

Informações Relacionadas

• Todas as versões do guia de configuração do Cisco Firepower Management Center podem ser encontradas aqui

Navegação na documentação do Cisco Secure Firewall Threat Defense

 Todas as versões do gerenciador de chassi do FXOS e dos guias de configuração da CLI podem ser encontradas aqui

Navegação na documentação FXOS do Cisco Firepower 4100/9300

 O Cisco Global Technical Assistance Center (TAC) recomenda enfaticamente este guia visual para conhecimento prático aprofundado sobre as tecnologias de segurança de

próxima geração Cisco Firepower:

<u>Cisco Firepower Threat Defense (FTD): práticas recomendadas de configuração e solução de problemas para o firewall de próxima geração (NGFW), o sistema de prevenção de invasão de próxima geração (NGIPS) e a proteção avançada contra malware (AMP)</u>

 Para todas as Notas técnicas de configuração e solução de problemas que pertencem às tecnologias Firepower

Cisco Secure Firewall Management Center

<u>Suporte Técnico e Documentação - Cisco Systems</u>

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.