## Configuración de la alta disponibilidad en FMC

## Contenido

ntroducción	
Prerequisites	
Requirements	
Componentes Utilizados	
Antecedentes	
Antes de comenzar	
Configurar	
Configuración del FMC secundario	
Configuración del FMC principal	
<u>/erificación</u>	

## Introducción

Este documento describe un ejemplo de configuración de alta disponibilidad (HA) en un centro de administración de firewall (FMC).

## Prerequisites

#### Requirements

No hay requisitos específicos para este documento.

#### **Componentes Utilizados**

La información de este documento se basa en el FMC seguro para VMware v7.2.5.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Los requisitos específicos para este documento incluyen:

- Ambos pares FMC deben estar en la misma versión de software, actualización de reglas de intrusión, base de datos de vulnerabilidades y paquete de seguridad ligero
- · Ambos pares FMC deben tener la misma capacidad o versión de hardware
- Ambos CSP requieren una licencia independiente

Para obtener un conjunto completo de requisitos, puede visitar la Guía de administración.



Advertencia: Si hay una discordancia en los requisitos enumerados, no puede configurar HA.

Este procedimiento es compatible con todos los dispositivos de hardware.

### Antes de comenzar

- · Garantizar el acceso del administrador a ambos CSP
- · Garantizar la conectividad entre interfaces de gestión
- Dedique unos instantes a revisar las versiones de software y asegúrese de que se han realizado todas las actualizaciones necesarias

## Configurar

### Configuración del FMC secundario

Paso 1. Inicie sesión en la interfaz gráfica de usuario (GUI) del dispositivo del FMC que va a asumir la función de secundario/en espera.



Inicio de sesión en FMC

#### Paso 2. Vaya a la pestaña Integración.

Firewall Management Center Overview / Dashboards / Dashboard	Overview	Analysis Policies	Devices	Objects	Integration	Deploy Q	🥝 🌣 🔞 admin	▼ dialia cisco SECURE
								Reporting
Summary Dashboard (switch 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 devices registered. Click here to register a device.		Cii	No Data No devices regi ck here to registe	istered. er a device.		Na Click h	No Data devices registered. ere to register a device	٥.
Last updated 3 minutes ago		Last updated 3 minutes	ago			Last updated 3 minutes ago		
Traffic by Application Risk	- ×							
	A	<ul> <li>Top Server Applie</li> </ul>	cations Seen		- ×	<ul> <li>Top Operating Syster</li> </ul>	ns Seen	- ×
No Data		1						

Vaya a la integración

Paso 3. Haga clic en Otras integraciones.

Integration	Deploy	Q 📀 🌣 🕜 admin 🕶 🖞	sco
SecureX Security Analytics & L Other Integrations	ogging	Intelligence Incidents Sources	
AMP		Elements Settings	
AMP Management Dynamic Analysis Cor	inections		

Navegar a otra integración

#### Paso 4. Acceda a la pestaña Alta Disponibilidad.

Firewall Integration	Manager Other Integr	nent Center ations / Cloud Services	Overview	Analysis	Policies	Devices	Objects	Integration	
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software	Manager On-Prem	

Vaya a Alta disponibilidad

#### Paso 5. Haga clic en Secundario.

Firewall Integration	Manager / Other Integ	ment Center rations / High Availabili	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹	0	¢	🕜 admin 🔻	cisco SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Srr	nart Software I	Manager On-Prem						Peer Manager
Select a role for	this Mana	gement Center and	specify peer detai	ls to setup hiç	gh availability	<i>ı</i> .								
Role For This Firev Standalone (N	wall Manager o High Avail:	ment Center: ability)												
O Primary														
<ul> <li>Secondary</li> </ul>														

Introduzca información y seleccione la función deseada para el CSP actual

Paso 6. Introduzca la información del par principal/activo y haga clic en 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.						



Nota: Tome nota de la clave de registro, ya que se utilizará en el CSP activo.

## Warning

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





Nota: Asegúrese de que no se esté ejecutando ninguna otra tarea mientras se crea HA, la GUI se reinicia.

Paso 8. Confirme que desea registrar el par principal.



Do you want to register primary peer: 10.18.19.31?





Advertencia: Toda la información sobre los dispositivos, la política o la configuración se eliminará de la FMC secundaria una vez que se cree HA.

Paso 9. Compruebe que el estado del CSP secundario está pendiente.

Firev Integra	vall Manage tion / Other Integ	ment Cen grations / Peer	ter Manager	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	≎	🕜 admin 🔻	alialia cisco	SECURE
Cloud Servi	ces Realms	Identity S	Sources	High Availability	eStreamer	Host Inp	ut Client	Smart Softwar	e Manager On-Prem							
Host			Last Modifi	ed			s	Status				S	tate			
10.18.19.31			2023-09-2	28 13:53:56			P	ending Registratio	n				0			1

#### Configuración del FMC principal

Repita los pasos 1 a 4 en el FMC principal/activo.

Paso 5. Haga clic en Primary.

Firewall N Integration / C	Managen Other Integr	nent Center ations / High Availabilit	Overview y	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	0	¢	🕜 admin 🔻	cisco SECURE
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client Si	mart Software I	Manager On-Prem						Peer Manager
Select a role for t	his Manag	ement Center and	specify peer detail	ls to setup hiç	gh availability	у.								
Role For This Firewa	all Managen High Availa	nent Center: bility)												
<ul> <li>Primary</li> </ul>														
Secondary														
Peer Details:														
Configure the secon After Firewall Manag	dary Manag gement Cer	gement Center with d iter high availability is	etails of the primary b configured in virtual of	pefore registrati or cloud enviror	ion. hment, each re	egistered Fire	wall Threat De	fense consumes an	additional Fire	power	MCv D	evice	license.	
Secondary Firewall	Managemei	nt Center Host:												
Registration Key*:														
Unique NAT ID:														
Register † Either host or NAT ID	is required.													

### Paso 6. Introduzca la información sobre el CSP secundario y haga clic en Registrar.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem	Peer Manager
Select a role for	this Manaş	gement Center and	specify peer detai	ls to setup hig	h availability.		
Role For This Firev	vall Manager o High Availa	nent Center: ibility)					
Primary							
Secondary							
Peer Details:							
Configure the second After Firewall Man Secondary Firewa 10.18.19.32	ondary Mana agement Cei II Manageme	gement Center with c nter high availability is nt Center Host:	letails of the primary t configured in virtual	pefore registration or cloud environ	on. Iment, each registerec	d Firewall Threat Defense consumes an additional Firepower MCv Device license.	
Registration Key*:							
cisco123							
Unique NAT ID:							
Register † Either host or NAT	D is required.						



Nota: Utilice la misma clave de registro utilizada como CSP secundario.

Paso 7. Esta advertencia le pide que confirme, haga clic en yes.

## Warning

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





Nota: Asegúrese de que no se está ejecutando ninguna otra tarea.

Paso 8. Confirme que desea registrarse en el FMC secundario.

# 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?





Nota: Asegúrese de que no hay información crítica sobre el CSP secundario, ya que al aceptar este mensaje se eliminan todas las configuraciones del CSP.

Sincronización entre los inicios primario y secundario; la duración depende de la configuración y de los dispositivos. Este proceso puede ser monitoreado desde ambas unidades.

	Firewall Integration /	Managen Other Integra	nent Cent ations / High A	er vailability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	Q	¢	🛿 admin 🕇	cisco SECURE
															Peer Manager
Cloud	Services	Realms	Identity Sou	rces	High Availability	eStreamer	Host Input	t Client Si	mart Software M	Manager On-Prer	m				
										Switch Peer Ro	oles 🏟	Break H/		II Pause Sy	nchronization
				High ava These op Database	ilability operations a perations include file e files synchronization	re in progress. The copy which may t on: 100% of 379Mi	e status messa ake time to co 8 transferred	ages and alerts omplete.	on this page are	e temporary. Pleas	e check after hig	h availabil	ty operat	ions are comple	te. ×
	Summa	ary						S	ystem Statu	IS					
	Status		A Tem	porarily	degraded- high ava	ailability operation p	ns are in rogress.			1	Local Active - Primary (10.18.19.31)	,	Stand	Remote Iby - Seconda (10.18.19.32)	ry
	Synchron	nization				4	Failed	c	perating Syste	m	7.2.5			7.2.5	
	Active S	ystem				10.1	8.19.31	s	oftware Versio	n	7.2.5-208			7.2.5-208	
	Standby	System				10.1	8.19.32	Ν	lodel	Secure	e Firewall Mana Center for VMwa	gement re	S Mana	ecure Firewall gement Center VMware	for



Nota: Mientras tiene lugar la sincronización, espere ver el estado como Error y Temporal degradado. Este estado se muestra hasta que se completa el proceso.

## Verificación

Una vez completada la sincronización, el resultado esperado es Status Healthy y Synchronization OK.

Firewall Integration	Manager / Other Integr	ment Center rations / High Availability	Overview	Analysis	Policies	Devices	Objects	Integration	Deploy	۹ (	\$	Ø admin ▼	diale SEC
													Peer Manage
ud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input	Client	Smart Software M	lanager On-Pre	m				
							4	Switch Peer R	oles 🔅 B	reak HA		II Pause Synd	chronization
Summ	ary					1	System Status	6					
Status				01	Healthy				Local		Stand	Remote	
Synchro	onization				OK				(10.18.19.31)		Stand (	10.18.19.32)	
Active \$	System			10.18	3.19.31		Operating System	n	7.2.5			7.2.5	
Standby	y System			10.18	3.19.32		Software Version		7.2.5-208			7.2.5-208	
							Model	Secur	re Firewall Manage Center for VMware	ment	Se Manag	ecure Firewall ement Center fo VMware	or

El Primario y el Secundario mantienen la sincronización; this is normal.

Firewall Management Center Integration / Other Integrations / High Availability	Devices Integration		۹ (	admin 🗸 👘 secure
				Peer Manager
Cloud Services High Availability eStreamer	Host Input Client			
		Switch	Peer Roles Break HA	II Pause Synchronization
0		0		
Summary		System Status		
Status	Synchronization task is in progress		Local Standby - Secondary	Remote
Synchronization	0 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

Dedique unos instantes a comprobar que los dispositivos se muestran correctamente en Primario y Secundario.

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).