

Configuración de la alta disponibilidad en FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Antes de comenzar](#)

[Configurar](#)

[Configuración del FMC secundario](#)

[Configuración del FMC principal](#)

[Verificación](#)

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.

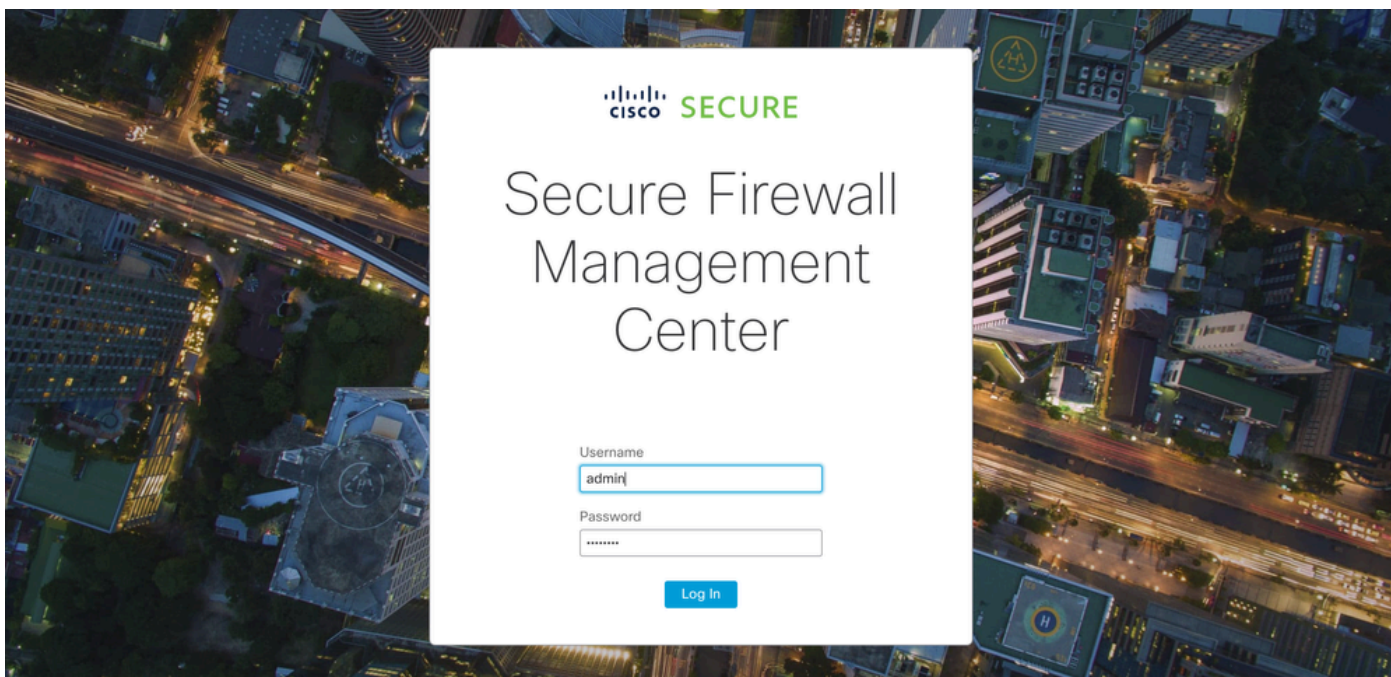
Antes de comenzar

- 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

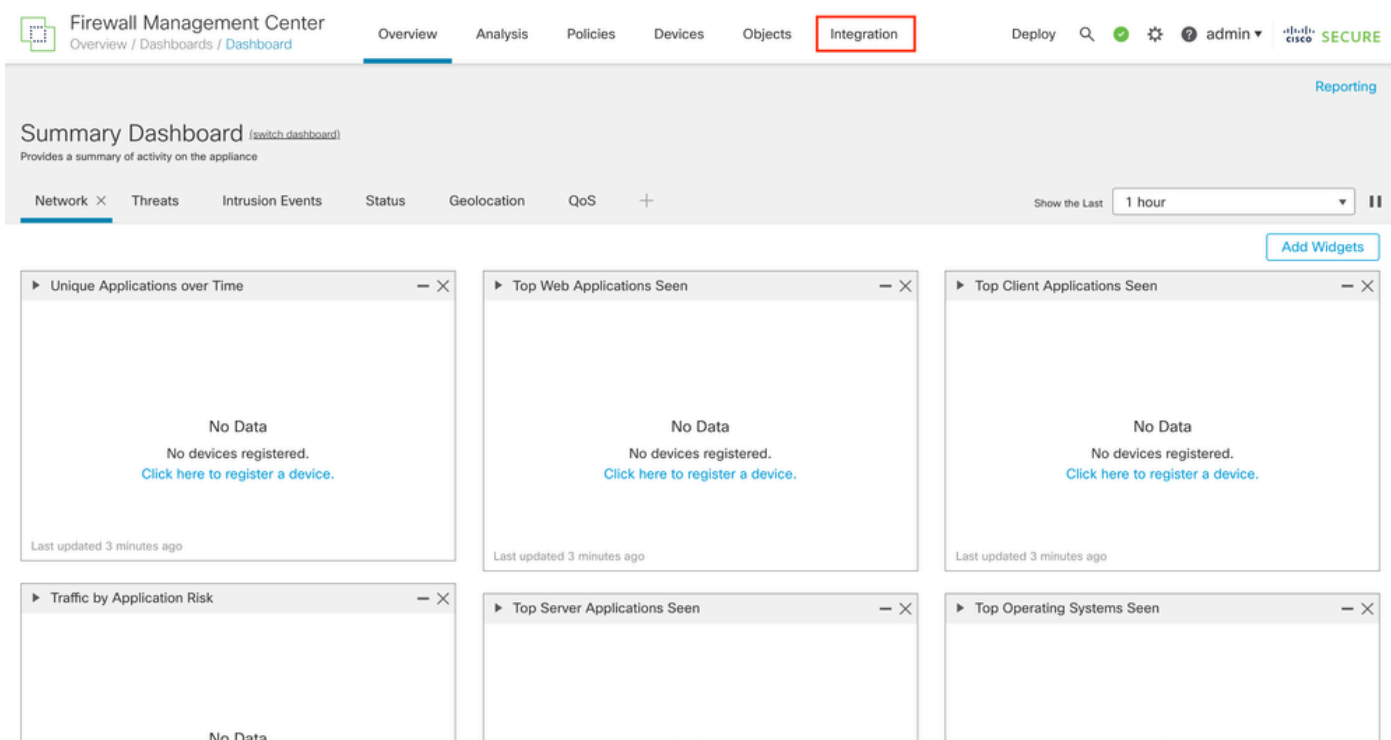
Configuración del FMC secundario

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.



Vaya a la integración

Paso 3. Haga clic en Otras integraciones.

SecureX

Security Analytics & Logging

Other Integrations

AMP

AMP Management

Dynamic Analysis Connections

Intelligence

Incidents

Sources

Elements

Settings

Navegar a otra integración

Paso 4. Acceda a la pestaña Alta Disponibilidad.



Firewall Management Center

Integration / Other Integrations / 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 Management Center

Integration / Other Integrations / High Availability

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

✔

⚙️

?

admin ▾

cisco SECURE

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

Peer Manager

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

Standalone (No High Availability)

Primary

Secondary

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.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

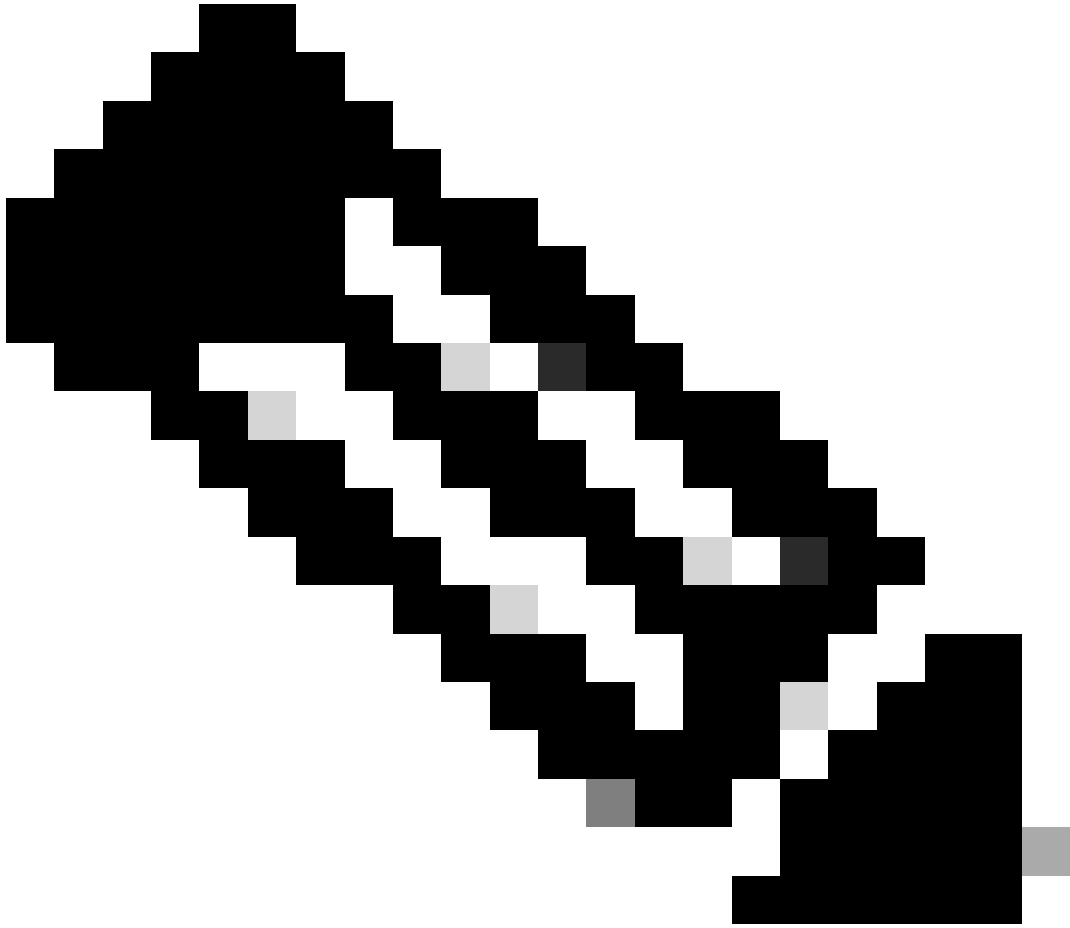
After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

† Either host or NAT ID is required.



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

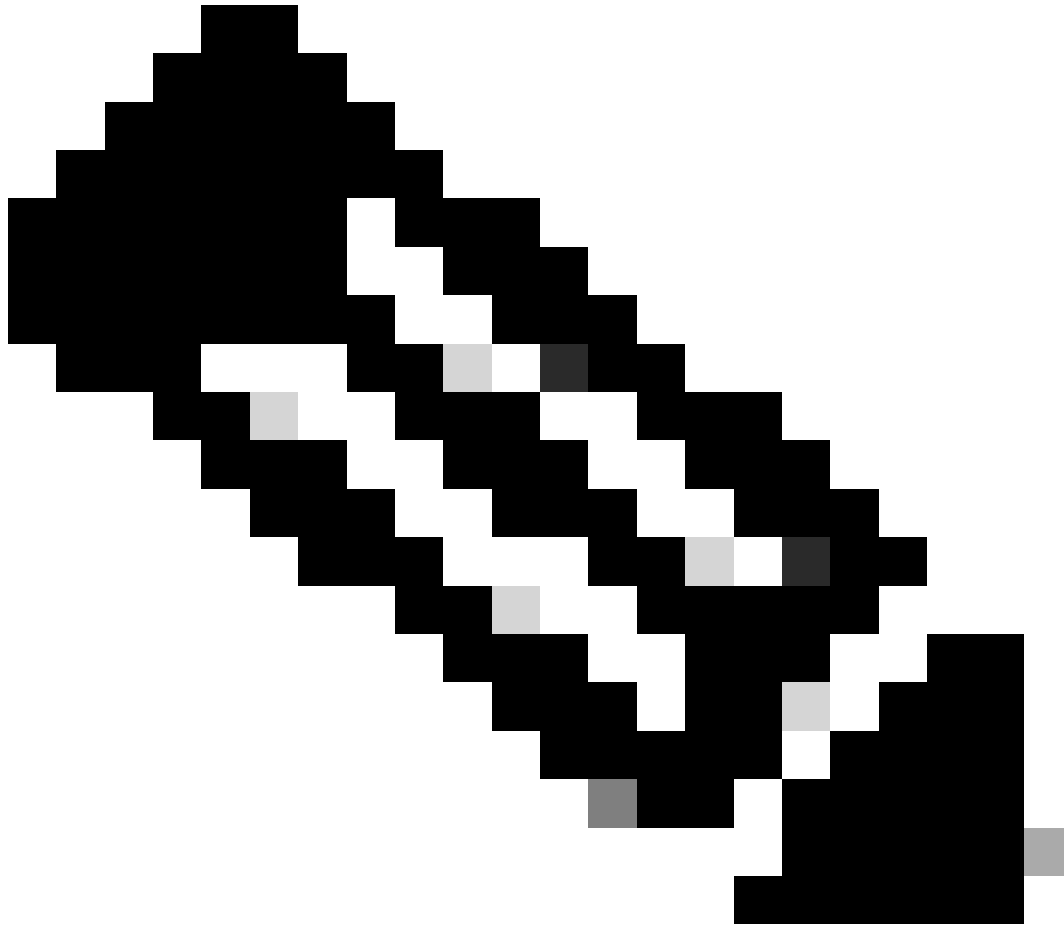
Paso 7. Esta advertencia le pide que confirme, haga clic en **Yes**.

Warning

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

No

Yes



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.

Warning

Do you want to register primary peer:
10.18.19.31?



No

Yes



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.

Host	Last Modified	Status	State	
10.18.19.31	2023-09-28 13:53:56	Pending Registration	<input checked="" type="checkbox"/>	 

Configuración del FMC principal

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

Paso 5. Haga clic en Primary.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

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.

Secondary Firewall Management 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.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

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.

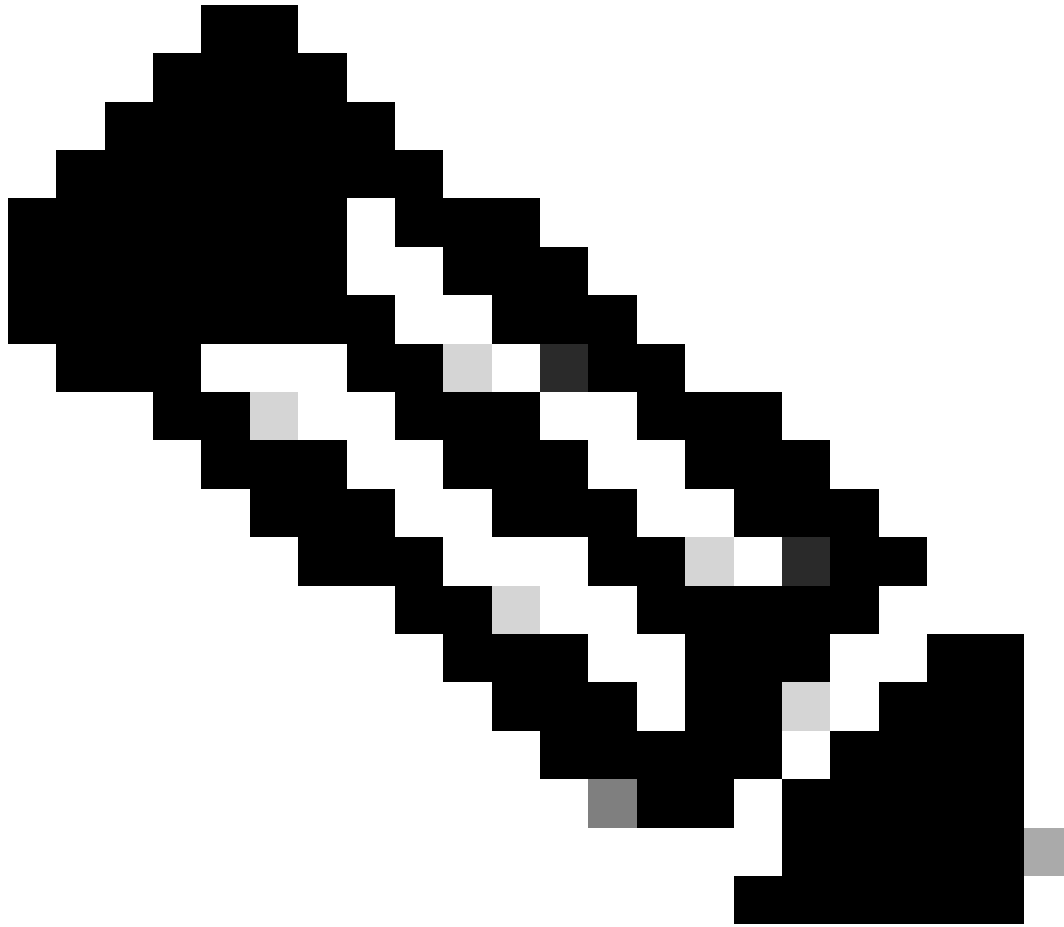
Secondary Firewall Management Center Host:

Registration Key*:

Unique NAT ID:

Register

† Either host or NAT ID is required.



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

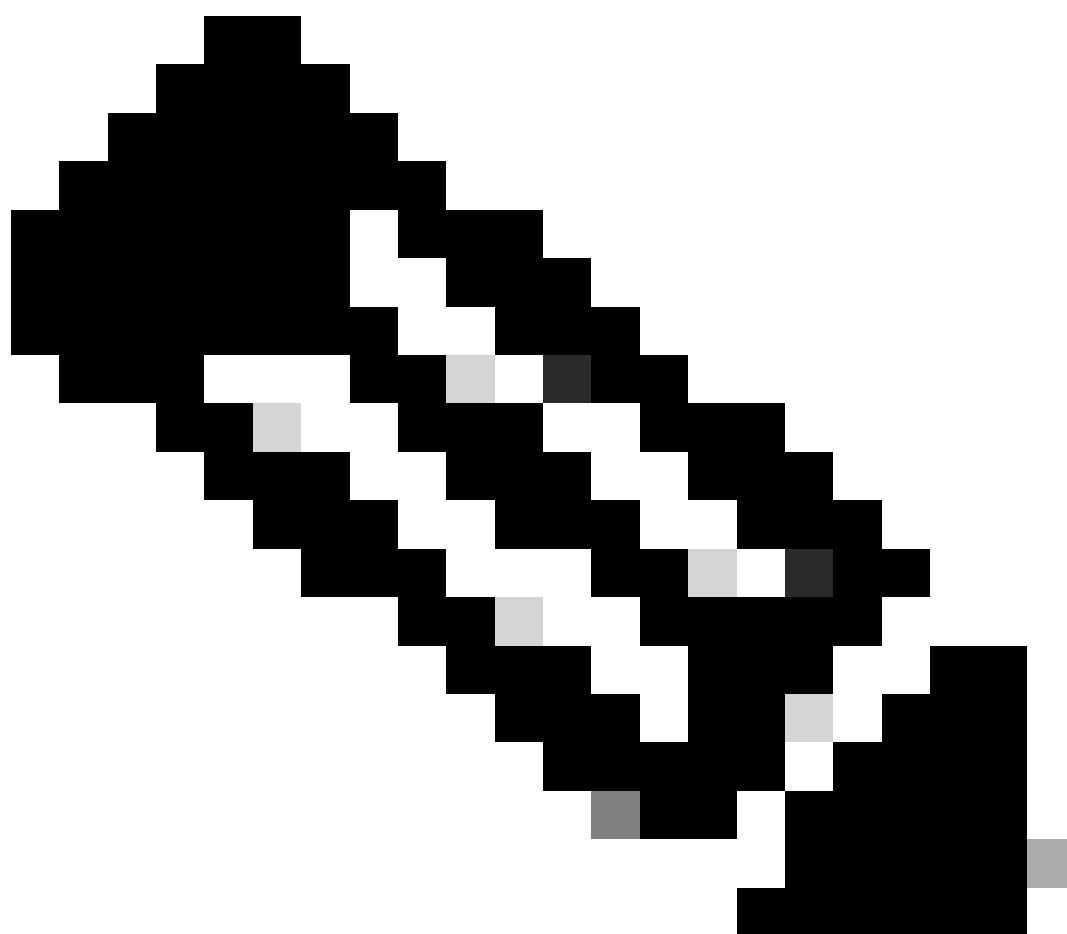
Paso 7. Esta advertencia le pide que confirme, haga clic en **Yes**.

Warning

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

No

Yes



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

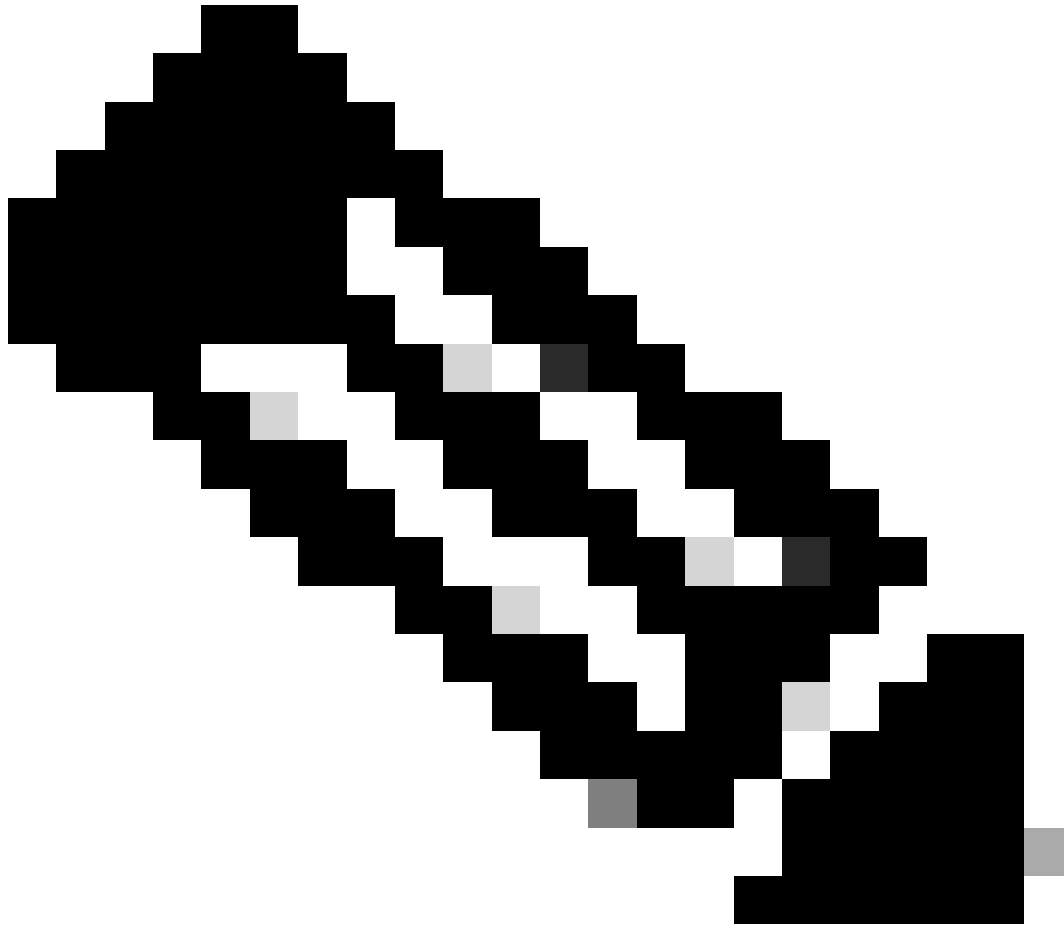
Paso 8. Confirme que desea registrarse en el FMC secundario.

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?

No

Yes



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.

Switch Peer Roles
Break HA
Pause Synchronization

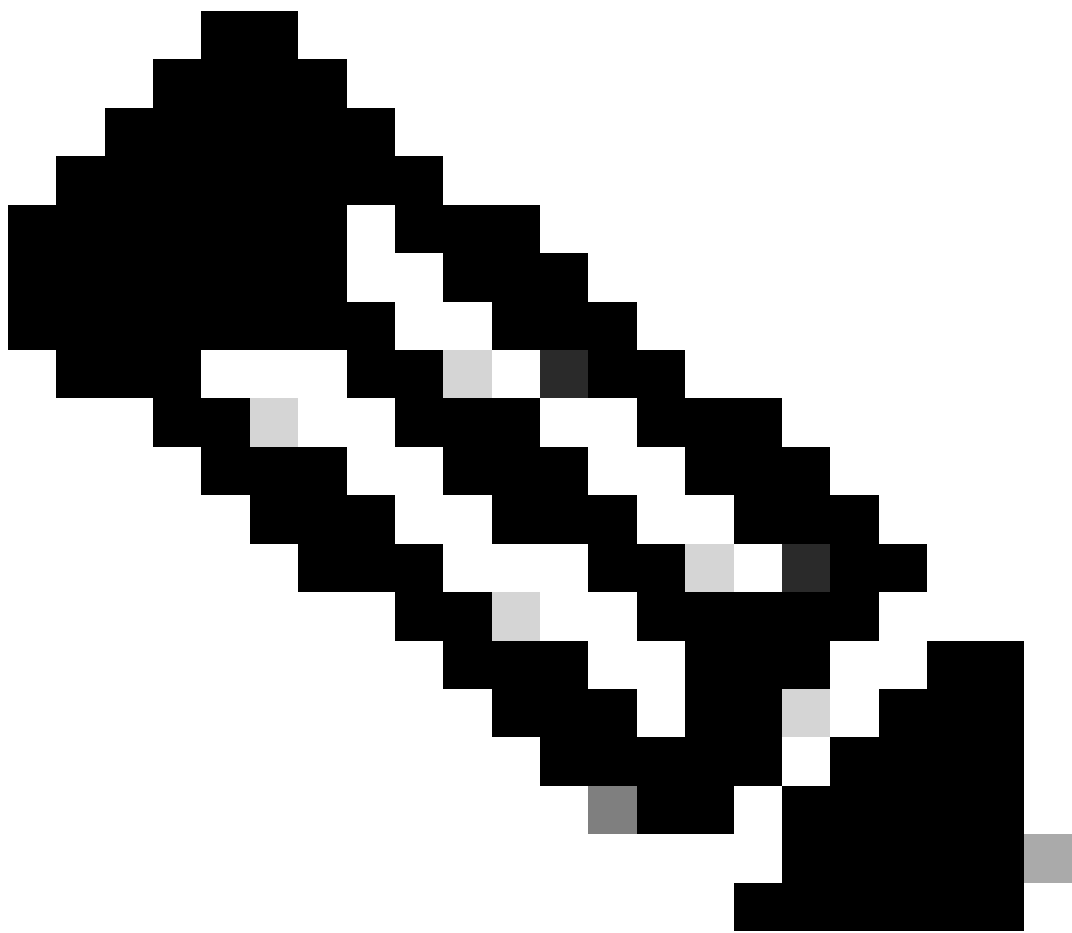
High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 379MB transferred

Summary

Status	▲ Temporarily degraded- high availability operations are in progress.
Synchronization	▲ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

System Status

	Local Active - Primary (10.18.19.31)	Remote Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware



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.

The screenshot shows the Firewall Management Center interface for High Availability. The 'Summary' section indicates a healthy status with synchronization OK. The 'System Status' table shows the local system as 'Active - Primary' and the remote system as 'Standby - Secondary'.

Summary	
Status	Healthy
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Active - Primary (10.18.19.31)	Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

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

The screenshot shows the Firewall Management Center interface for High Availability. The 'Summary' section indicates that the synchronization task is in progress. The 'System Status' table shows the local system as 'Standby - Secondary' and the remote system as 'Active - Primary'.

Summary	
Status	Synchronization task is in progress
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Standby - Secondary (10.18.19.32)	Active - Primary (10.18.19.31)
Operating System	7.2.5	7.2.5
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).