

Sustitución de Secure Firewall Management Center en un par HA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Solución 1](#)

[Proceso para reemplazar una unidad defectuosa por una de respaldo](#)

[Solución 2](#)

[Proceso para reemplazar una unidad defectuosa sin respaldo](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo reemplazar un Secure Firewall Management Center defectuoso en un par de alta disponibilidad (HA).

Prerequisites

Requirements

Cisco recomienda que conozca este tema:

- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall Management Center (FMC) que ejecuta la versión 7.2.5 (1) en modo HA

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,

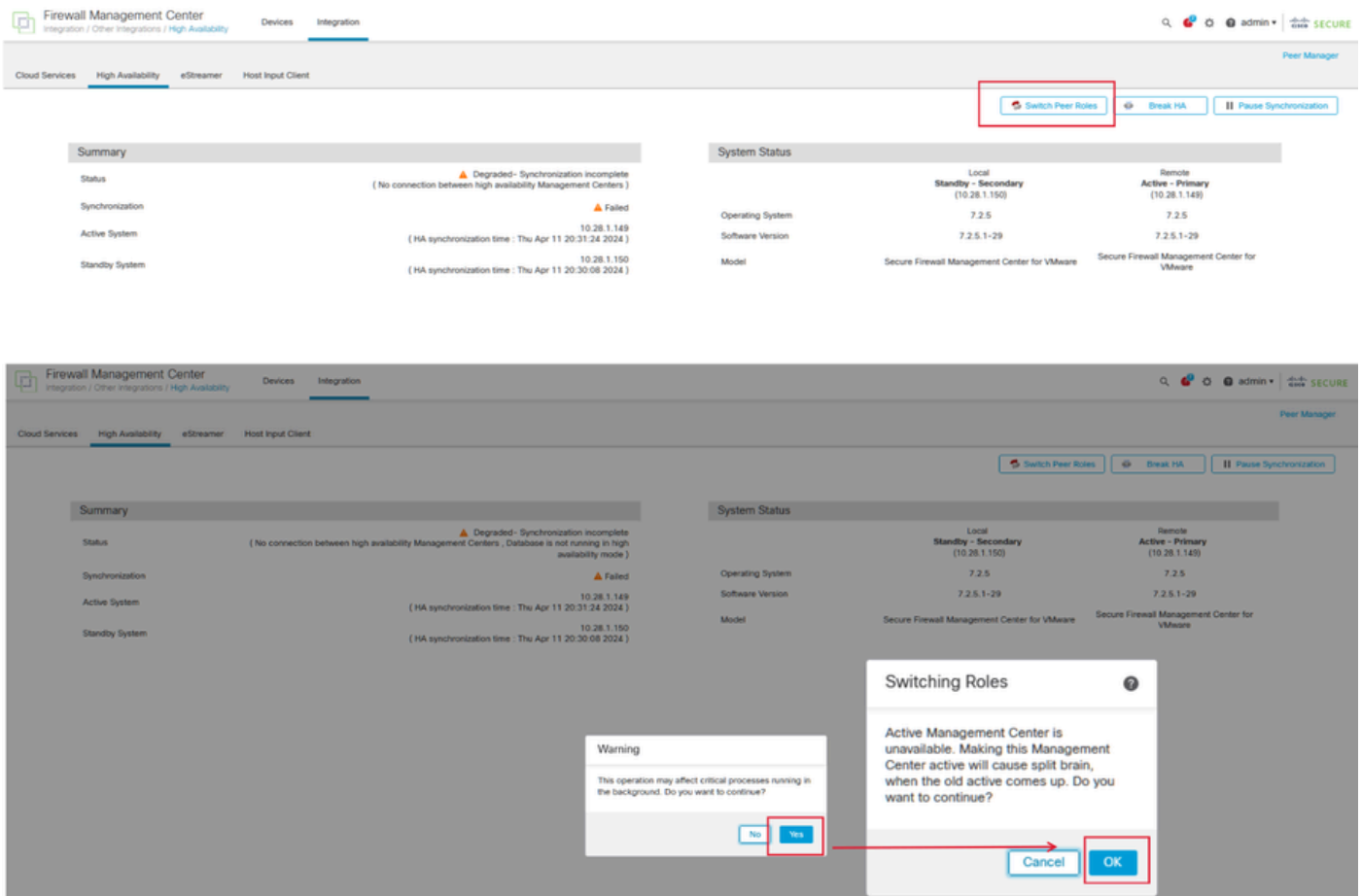
asegúrese de entender el posible impacto de cualquier comando.

Configurar

Solución 1

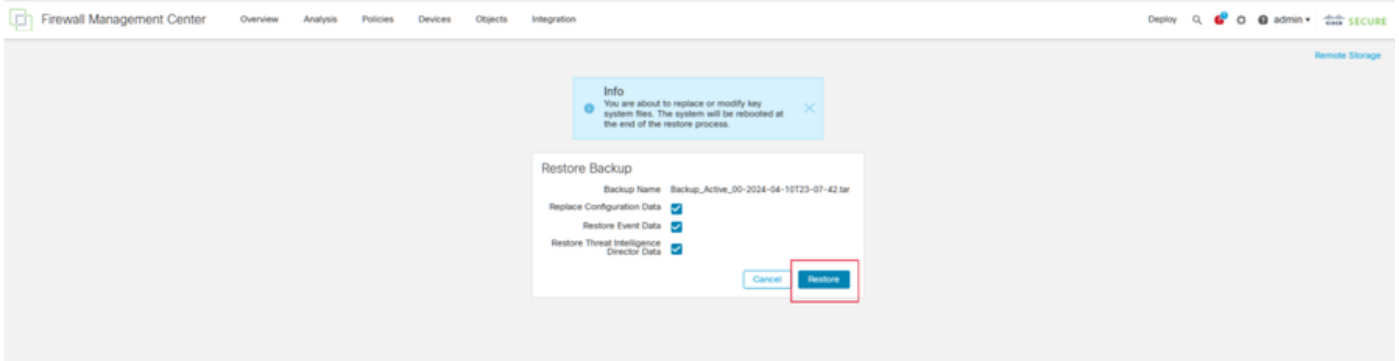
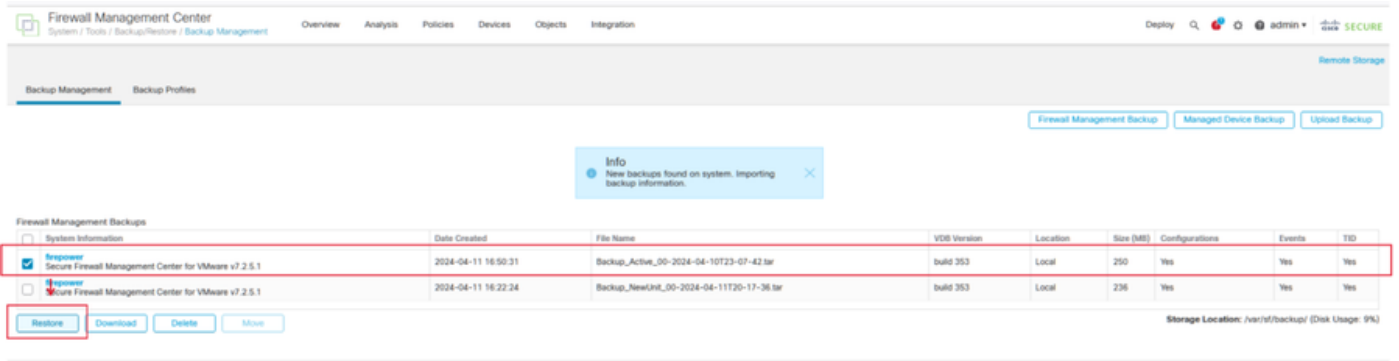
Proceso para reemplazar una unidad defectuosa por una de respaldo

Paso 1: Asigne la unidad operativa como activa. Para obtener más información, consulte [Switching Peers en el par de alta disponibilidad de Management Center.](#)



Paso 2: Vuelva a crear una imagen de la nueva unidad para que coincida con la versión de software de la unidad activa. Consulte [Recreación de la Imagen de un Modelo de Hardware de Cisco Secure Firewall Management Center](#) para obtener más información.

Paso 3: Restaure la copia de seguridad de datos de la unidad defectuosa en el nuevo centro de gestión. Navegue hasta Sistema > Copia de seguridad/Restauración, cargue el archivo de copia de seguridad y restáurelo a la nueva unidad.



Paso 4: Si es necesario, actualice la misma versión de las actualizaciones de la base de datos de geolocalización (GeoDB), de la base de datos de vulnerabilidades (VDB) y del software del sistema como la unidad activa para garantizar la coherencia.

Active Unit

New Unit



Paso 5: Una vez que se completan las actualizaciones, ambas unidades pueden mostrar un estado activo, lo que puede llevar a una condición de cerebro dividido HA.

Paso 6: Proceda a configurar manualmente la unidad que ha estado en funcionamiento continuo como activa. Esto le permite sincronizar la configuración más reciente con la unidad de sustitución.

The screenshot shows the Firewall Management Center interface in a split brain state. A notification at the top states: "This high availability pair is in split brain. Make one Management Center active by clicking 'Make Me Active'." The interface is divided into two main sections: Summary and System Status.

Summary:

- Status: **Split Brain - Management Center is active on both peers. (Database is not configured for high availability)**
- Synchronization: **Failed** (HA synchronization time: Thu Apr 11 21:03:25 2024)
- Active System: 10.28.1.150 (HA synchronization time: Thu Apr 11 21:03:00 2024)
- Standby System: 10.28.1.149 (HA synchronization time: Thu Apr 11 21:03:00 2024)

System Status:

	Local Split Brain - Secondary (10.28.1.150)	Remote Split Brain - Primary (10.28.1.149)
Operating System	7.2.5	7.2.5
Software Version	7.2.5.1-29	7.2.5.1-29
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

A "Warning" dialog box is displayed, stating: "This operation may affect critical processes running in the background. The local peer will be active and the other peer will become a standby. The active peer will overwrite configuration and policies present on the standby peer. Do you want to continue?" with "No" and "Yes" buttons.

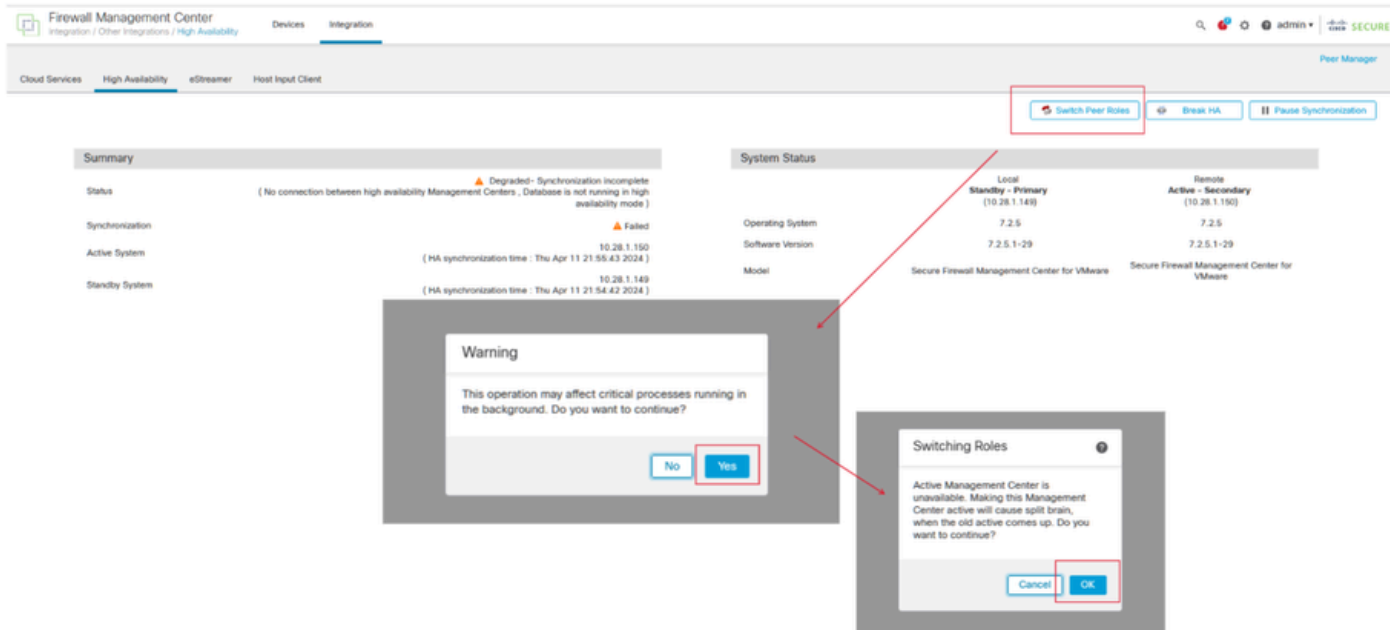
A "Make Me Active" dialog box is also shown, asking: "Do you want to make this Management Center active and peer standby?" with "Cancel" and "OK" buttons. A red arrow points from the "Yes" button in the warning dialog to the "OK" button in the "Make Me Active" dialog.

Paso 7: Si la sincronización es exitosa, lo que puede tomar algún tiempo, navegue hasta la interfaz web de la unidad activa. A continuación, modifique las funciones y posicione la nueva unidad como el dispositivo activo.

Solución 2

Proceso para reemplazar una unidad defectuosa sin respaldo

Paso 1: Asigne la unidad operativa como activa. Para obtener más información, consulte [Switching Peers en el par de alta disponibilidad de Management Center.](#)



Paso 2: Vuelva a crear una imagen de la nueva unidad para que coincida con la versión de software de la unidad activa. Consulte [Recreación de la Imagen de un Modelo de Hardware de Cisco Secure Firewall Management Center](#) para obtener más información.

Paso 3: Si es necesario, actualice la misma versión de las actualizaciones de la base de datos de geolocalización (GeoDB), de la base de datos de vulnerabilidades (VDB) y del software del sistema como la unidad activa para garantizar la coherencia.

Operational Unit

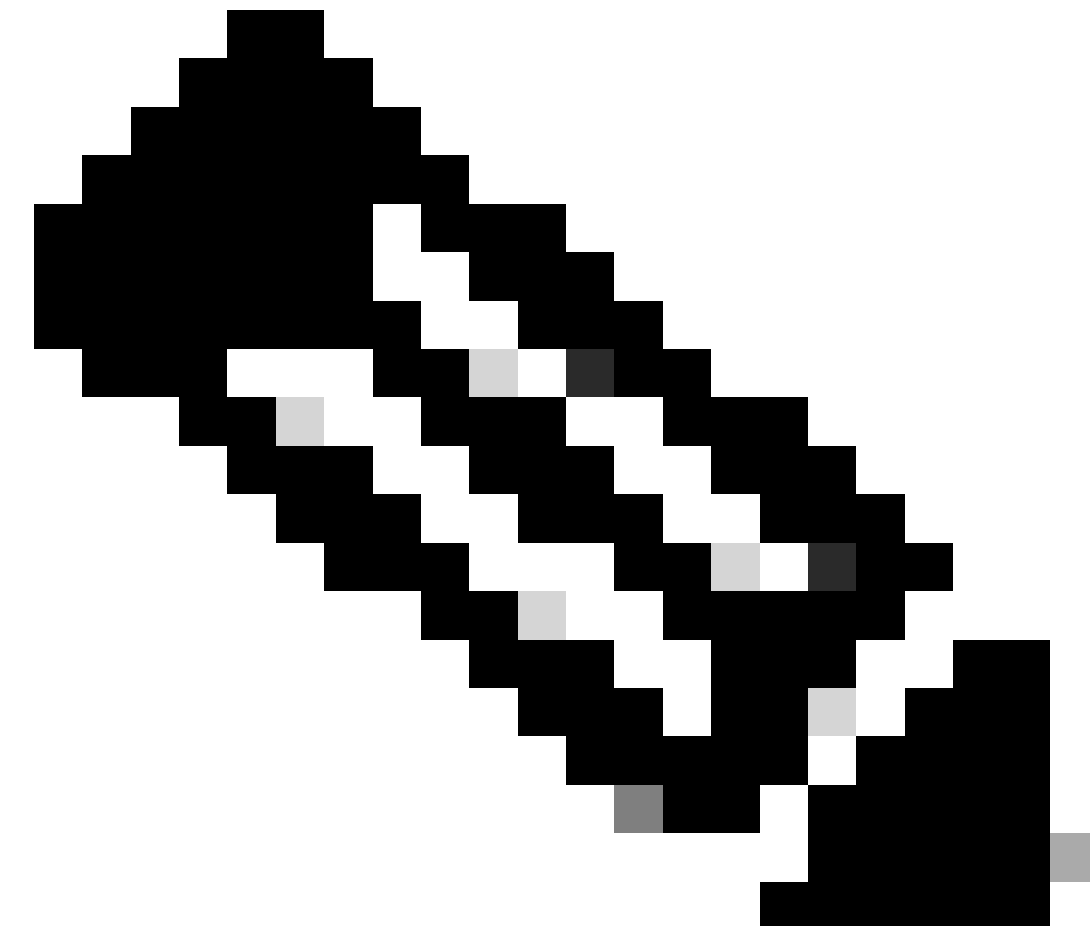
Replacement



Paso 4: Utilice la interfaz web del centro de gestión activo para interrumpir el HA. Cuando se le solicite, seleccione la opción Administrar dispositivos registrados desde esta consola.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'High Availability' section is active, showing a 'Summary' and 'System Status' panel. The 'Break HA' button is highlighted with a red box. A dialog box titled 'Break HA' is open, asking 'How do you want to manage devices after breaking high availability?' with three radio button options: 'Manage registered devices from this console' (selected and highlighted with a red box), 'Manage registered devices from peer console', and 'Stop managing registered devices from both consoles'. The 'OK' button is also highlighted with a red box.

Paso 5: Reconfigure el HA del centro de gestión configurando el centro de gestión operativa como principal y la unidad de sustitución como secundaria. Para obtener instrucciones detalladas, consulte [Establecimiento de la alta disponibilidad de Management Center](#).



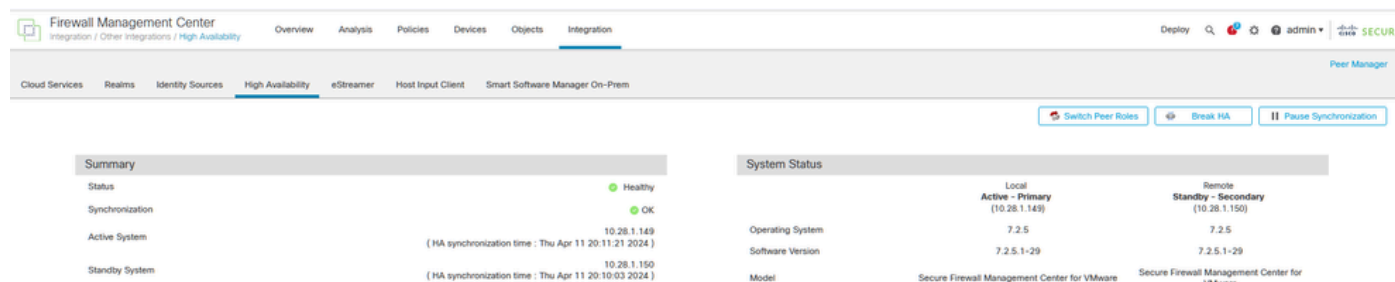
Nota: cuando se restablece HA, la configuración más reciente del centro de gestión principal se sincroniza con el centro de gestión secundario. Las licencias Classic y Smart

están diseñadas para integrarse sin problemas.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

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



Summary	
Status	Healthy
Synchronization	OK
Active System	10.28.1.149 (HA synchronization time : Thu Apr 11 20:11:21 2024)
Standby System	10.28.1.150 (HA synchronization time : Thu Apr 11 20:10:03 2024)

System Status		
	Local	Remote
	Active - Primary (10.28.1.149)	Standby - Secondary (10.28.1.150)
Operating System	7.2.5	7.2.5
Software Version	7.2.5.1-29	7.2.5.1-29
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Dado que este proceso puede tardar algún tiempo, las unidades Primaria y Secundaria aún se están sincronizando. Durante este período, asegúrese de comprobar que los dispositivos están correctamente enumerados en las unidades primaria y secundaria.

Además, se puede realizar la verificación a través de la CLI. Esto se logra conectándose a la CLI, cambiando al modo experto, elevando los privilegios y ejecutando estas secuencias de comandos:

```
<#root>
```

```
fmc1:/Volume/home/admin#
```

```
troubleshoot_HADC.pl
```

```
***** Troubleshooting Utility *****
```

- 1 Show HA Info Of FMC
- 2 Execute Sybase DBPing
- 3 Show Arbiter Status
- 4 Check Peer Connectivity
- 5 Print Messages of AQ Task
- 6 Show FMC HA Operations History (ASC order)
- 7 Dump To File: FMC HA Operations History (ASC order)
- 8 Last Successful Periodic Sync Time (When it completed)
- 9 Print HA Status Messages
- 10 Compare active and standby device list
- 11 Check manager status of standby missing devices
- 12 Check critical PM processes details
- 13 Help
- 0 Exit

```
*****
```

<#root>

fmc1:/Volume/home/admin#

troubleshoot_HADC.pl

***** Troubleshooting Utility *****

1 Show HA Info Of FMC

2 Execute Sybase DBPing

3 Show Arbiter Status

4 Check Peer Connectivity

5 Print Messages of AQ Task

6 Show FMC HA Operations History (ASC order)

7 Dump To File: FMC HA Operations History (ASC order)

8 Help

0 Exit

Para obtener información más detallada, consulte [Verificación del modo de Firepower, la instancia, la alta disponibilidad y la configuración de escalabilidad.](#)

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Guía de administración de Cisco Secure Firewall Management Center, 7.4. Alta disponibilidad](#)
- [Soporte técnico y descargas de Cisco](#)

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).