

Remplacement du centre de gestion de pare-feu sécurisé dans une paire HA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Solution 1](#)

[Processus de remplacement d'une unité défectueuse par une unité de secours](#)

[Solution 2](#)

[Processus de remplacement d'une unité défectueuse sans sauvegarde](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment remplacer un centre de gestion de pare-feu sécurisé défectueux dans une paire haute disponibilité (HA).

Conditions préalables

Exigences

Cisco vous recommande de connaître cette rubrique :

- Cisco Secure Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center (FMC) exécutant la version 7.2.5 (1) en mode haute disponibilité

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Solution 1

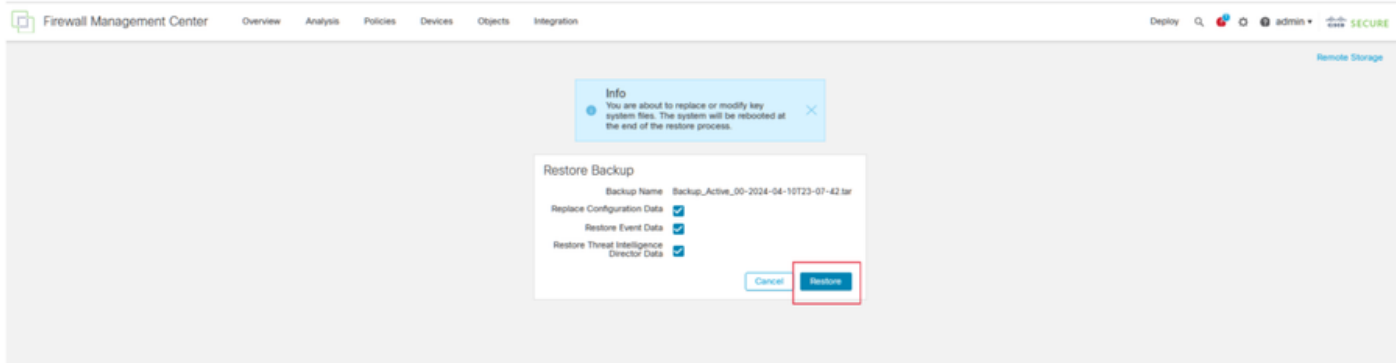
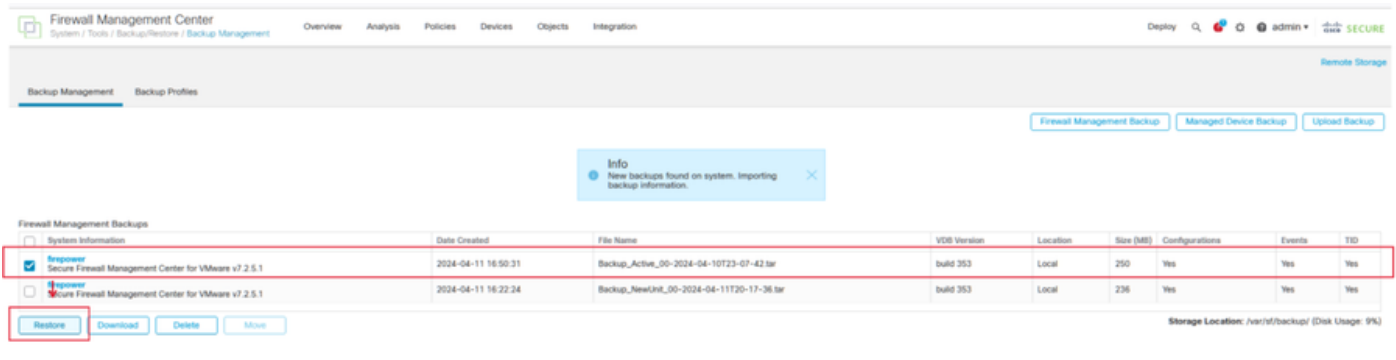
Processus de remplacement d'une unité défectueuse par une unité de secours

Étape 1 : Attribuez l'unité opérationnelle comme étant active. Pour plus d'informations, référez-vous à [Homologues de commutation dans la paire haute disponibilité de Management Center](#).

The screenshot displays the Firewall Management Center interface. The top navigation bar includes 'Firewall Management Center', 'Integration / Other Integrations / High Availability', 'Devices', and 'Integration'. The main content area is divided into two columns: 'Summary' and 'System Status'. The 'Summary' panel shows a 'Degraded - Synchronization incomplete' status with a warning icon. The 'System Status' panel shows details for 'Local Standby - Secondary' and 'Remote Active - Primary'. A red box highlights the 'Switch Peer Roles' button in the top right corner. Below the main content, a 'Switching Roles' dialog box is shown, containing a 'Warning' message: 'This operation may affect critical processes running in the background. Do you want to continue?'. The 'Yes' button in the warning dialog and the 'OK' button in the 'Switching Roles' dialog are highlighted with red boxes.

Étape 2 : Réinstallez la nouvelle unité pour qu'elle corresponde à la version logicielle de l'unité active. Référez-vous à [Réinstaller un modèle matériel d'un Cisco Secure Firewall Management Center](#) pour plus d'informations.

Étape 3 : restaurez la sauvegarde des données de l'unité défailante vers le nouveau centre de gestion. Accédez à System > Backup/Restore, téléchargez le fichier de sauvegarde et restaurez-le sur la nouvelle unité.



Étape 4 : Si nécessaire, mettez à jour la même version des mises à jour de la base de données de géolocalisation (GeoDB), de la base de données de vulnérabilités (VDB) et des mises à jour du logiciel système que l'unité active afin d'assurer la cohérence.

Active Unit

New Unit



Étape 5 : Une fois les mises à jour terminées, les deux unités peuvent afficher un état actif, ce qui peut conduire à un état de cerveau divisé HA.

Étape 6 : passez à la configuration manuelle de l'unité qui a été continuellement opérationnelle comme étant active. Cela lui permet de synchroniser la dernière configuration avec l'unité de remplacement.

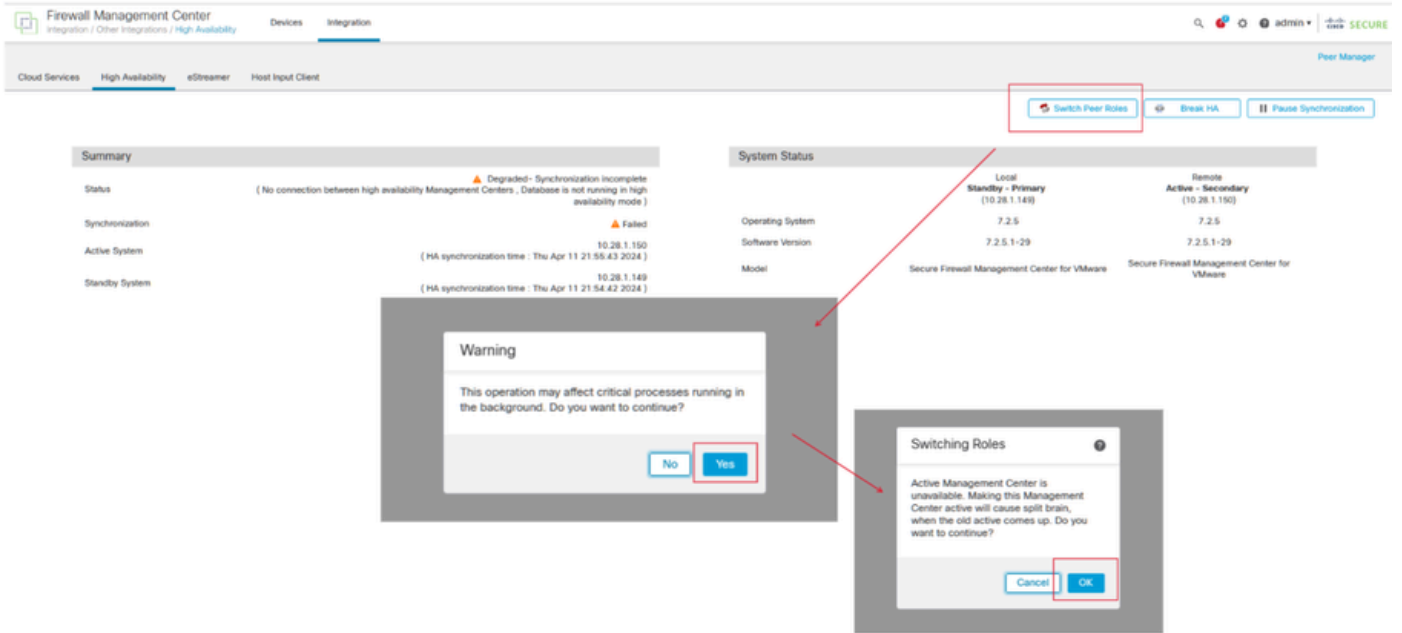
The screenshot shows the Firewall Management Center interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and Integration. Below this, there are sub-tabs: Cloud Services, Realms, Identify Sources, High Availability, eStreamer, Host Input Client, and Smart Software Manager On-Prem. A 'Peer Manager' button is visible on the right. A red box highlights the 'Make Me Active' button. A message states: 'This high availability pair is in split brain. Make one Management Center active by clicking 'Make Me Active'.' Below this, there are two panels: 'Summary' and 'System Status'. The 'Summary' panel shows a warning: 'Split Brain - Management Center is active on both peers. (Database is not configured for high availability)'. It also shows synchronization status: 'Failed' with a synchronization time of 'Thu Apr 11 21:03:25 2024'. The 'System Status' panel shows details for the local and remote peers, including Operating System (7.2.5), Software Version (7.2.5.1-29), and Model (Secure Firewall Management Center for VMware). A 'Make Me Active' dialog box is open, asking: 'Do you want to make this Management Center active and peer standby?'. It has 'Cancel' and 'OK' buttons. A 'Warning' dialog box is also visible, 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?'. It has 'No' and 'Yes' buttons. A red arrow points from the 'Yes' button to the 'OK' button in the 'Make Me Active' dialog.

Étape 7 : Une fois la synchronisation réussie, ce qui peut prendre un certain temps, accédez à l'interface Web de l'unité active. Modifiez ensuite les rôles, en positionnant la nouvelle unité en tant qu'appliance active.

Solution 2

Processus de remplacement d'une unité défectueuse sans sauvegarde

Étape 1 : Attribuez l'unité opérationnelle comme étant active. Pour plus d'informations, référez-vous à [Homologues de commutation dans la paire haute disponibilité de Management Center.](#)



Étape 2 : Réinstallez la nouvelle unité pour qu'elle corresponde à la version logicielle de l'unité active. Référez-vous à [Réinstaller un modèle matériel d'un Cisco Secure Firewall Management Center](#) pour plus d'informations.

Étape 3 : Si nécessaire, mettez à jour la même version des mises à jour de la base de données de géolocalisation (GeoDB), de la base de données de vulnérabilités (VDB) et des mises à jour du logiciel système que l'unité active afin d'assurer la cohérence.

Operational Unit

Replacement



Étape 4 : utilisez l'interface Web du centre de gestion actif pour interrompre la haute disponibilité. Lorsque vous y êtes invité, sélectionnez l'option Manage registered devices à partir de cette console.

Firewall Management Center
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin • SECURE

Peer Manager

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

Switch Peer Roles Break HA Pause Synchronization

Summary

Status (No connection between high availability Management Centers, Database is not configured for high availability) **Degraded - Synchronization incomplete**

Synchronization **Failed**

Active System (HA synchronization time: 10.28.1.149)

Standby System (HA synchronization time: ...)

System Status

	Local	Remote
Active - Primary (10.28.1.149)	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
	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Break HA

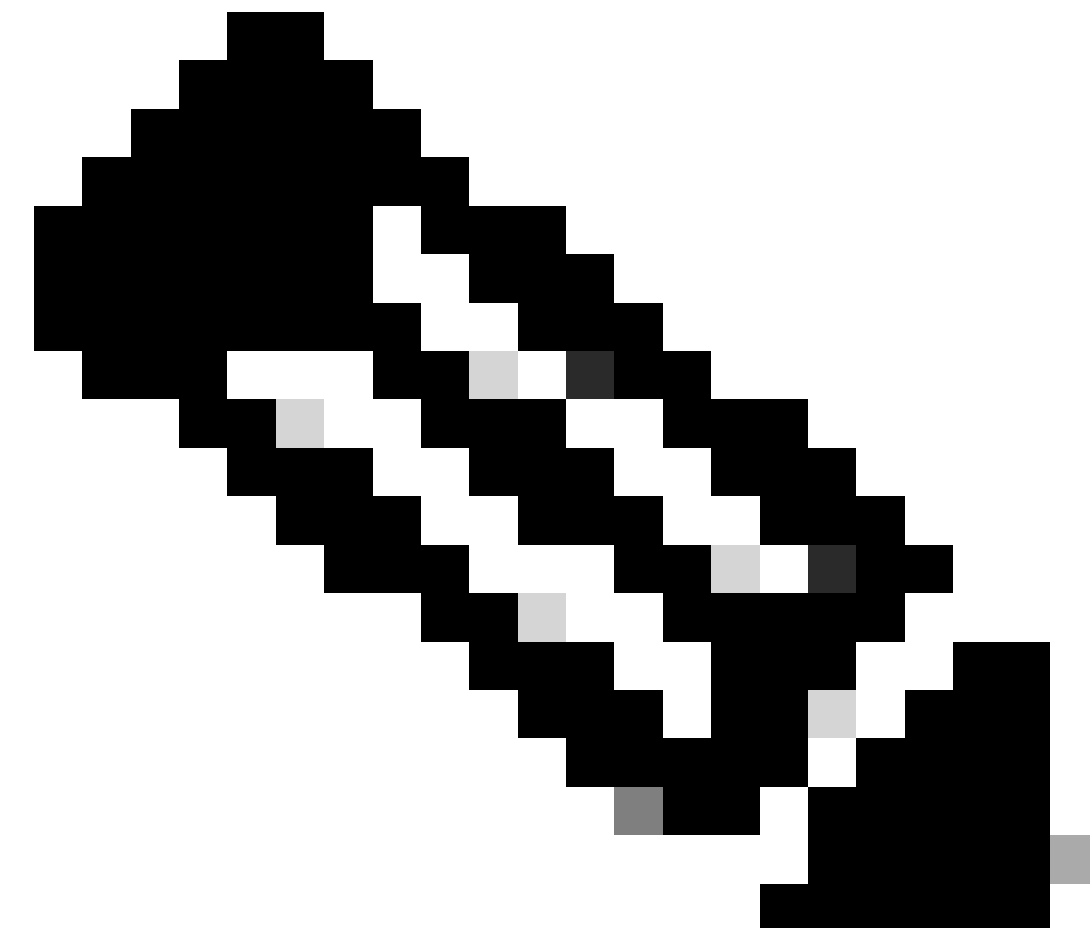
How do you want to manage devices after breaking high availability?

- Manage registered devices from this console.
- Manage registered devices from peer console.
- Stop managing registered devices from both consoles.

All devices will be unregistered from peer console.

Cancel OK

Étape 5 : Reconfigurez la haute disponibilité du centre de gestion en configurant le centre de gestion opérationnel comme principal et l'unité de remplacement comme secondaire. Pour obtenir des instructions détaillées, consultez [Établissement de la haute disponibilité de Management Center](#).



Remarque : lorsque la haute disponibilité est rétablie, la dernière configuration du centre

de gestion principal est synchronisée avec celle du centre de gestion secondaire. Les licences Classic et Smart sont conçues pour s'intégrer facilement.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois la synchronisation terminée, le résultat attendu est Status Healthy et 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

Ce processus pouvant prendre un certain temps, les unités principale et secondaire sont toujours en cours de synchronisation. Pendant cette période, assurez-vous que vos périphériques sont correctement répertoriés sur les unités principale et secondaire.

En outre, la vérification peut être effectuée via l'interface de ligne de commande. Pour ce faire, connectez-vous à l'interface de ligne de commande, passez en mode expert, augmentez les privilèges et exécutez les scripts suivants :

```
<#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

Pour plus d'informations, consultez [Vérifier le mode Firepower, l'instance, la haute disponibilité et la configuration de l'évolutivité.](#)

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Guide d'administration de Cisco Secure Firewall Management Center, 7.4. Haute disponibilité](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.