

Sostituzione di Secure Firewall Management Center in una coppia HA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Soluzione 1](#)

[Procedura per la sostituzione di un'unità difettosa con un backup](#)

[Soluzione 2](#)

[Procedura per la sostituzione di un'unità difettosa senza backup](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come sostituire un centro di gestione Secure Firewall difettoso in una coppia ad alta disponibilità (HA).

Prerequisiti

Requisiti

Cisco consiglia di conoscere questo argomento:

- Cisco Secure Firewall Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Management Center (FMC) con versione 7.2.5 (1) in modalità HA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Soluzione 1

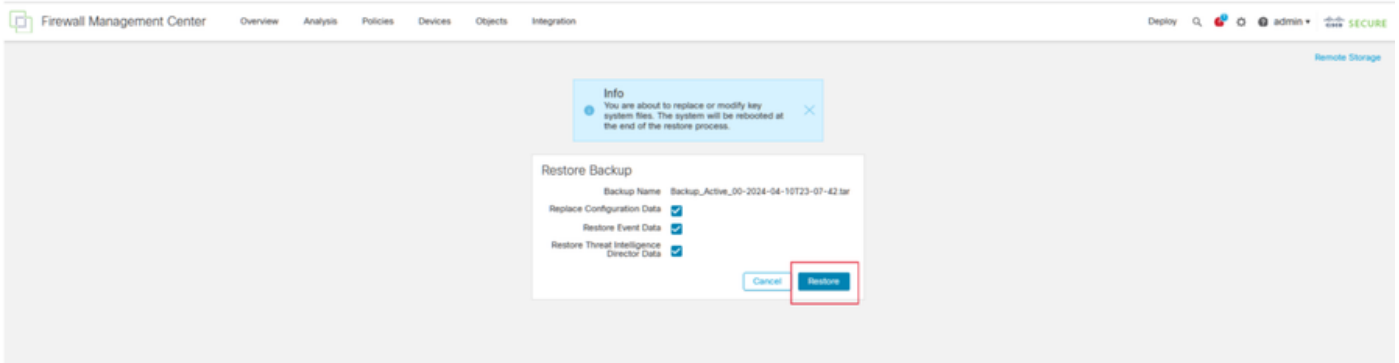
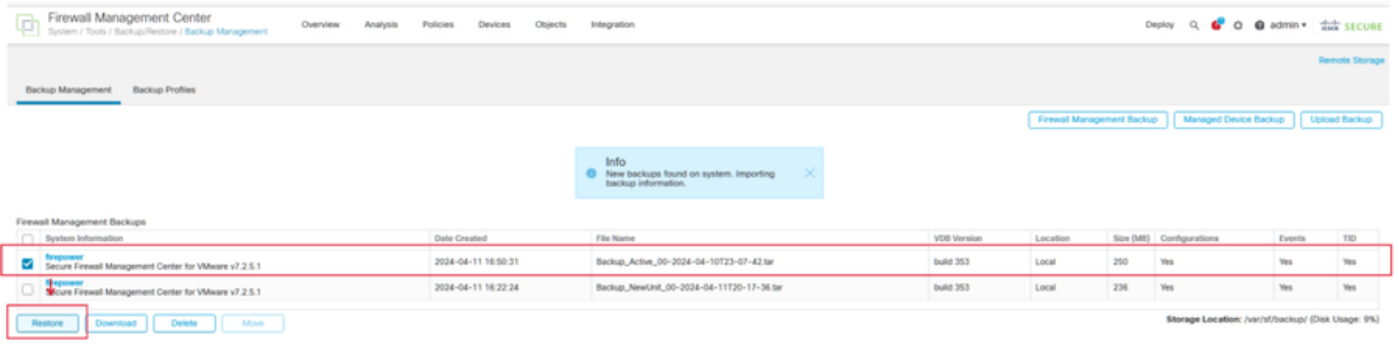
Procedura per la sostituzione di un'unità difettosa con un backup

Passo 1: Assegnare l'unità operativa come attiva. Per ulteriori informazioni, fare riferimento a [Switching Peer in Management Center High Availability Pair.](#)

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' column shows the status of the high availability pair, including 'Status', 'Synchronization', 'Active System', and 'Standby System'. The 'System Status' column shows details for the 'Local Standby - Secondary' and 'Remote Active - Primary' units, including 'Operating System', 'Software Version', and 'Model'. A 'Switch Peer Roles' button is highlighted with a red box. Below the main content, a 'Warning' dialog box is shown with the 'Yes' button highlighted, and a 'Switching Roles' dialog box is shown with the 'OK' button highlighted.

Passaggio 2: ricreare l'immagine della nuova unità in modo che corrisponda alla versione software dell'unità attiva. per ulteriori informazioni, fare riferimento a [Reimage a Hardware Model of a Cisco Secure Firewall Management Center](#) (Ricrea immagine di un modello hardware di un Cisco Secure Firewall Management Center).

Passaggio 3: Ripristinare il backup dei dati dall'unità guasta al nuovo centro di gestione. Selezionare Sistema > Backup/Ripristino, caricare il file di backup e ripristinarlo sulla nuova unità.



Passo 4: se necessario, aggiornare la stessa versione degli aggiornamenti del database di geolocalizzazione (GeoDB), degli aggiornamenti del database di vulnerabilità (VDB) e degli aggiornamenti software di sistema dell'unità attiva per garantire la coerenza.

Active Unit

New Unit



Passaggio 5: Una volta completati gli aggiornamenti, entrambe le unità possono visualizzare uno stato attivo, che può portare a una condizione di split-brain HA.

Passaggio 6: procedere con l'impostazione manuale dell'unità operativa in modo continuativo come attiva. Ciò consente di sincronizzare la configurazione più recente con l'unità sostitutiva.

The screenshot shows the Firewall Management Center interface with a split brain state. A warning message 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 a Summary section and a System Status section.

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

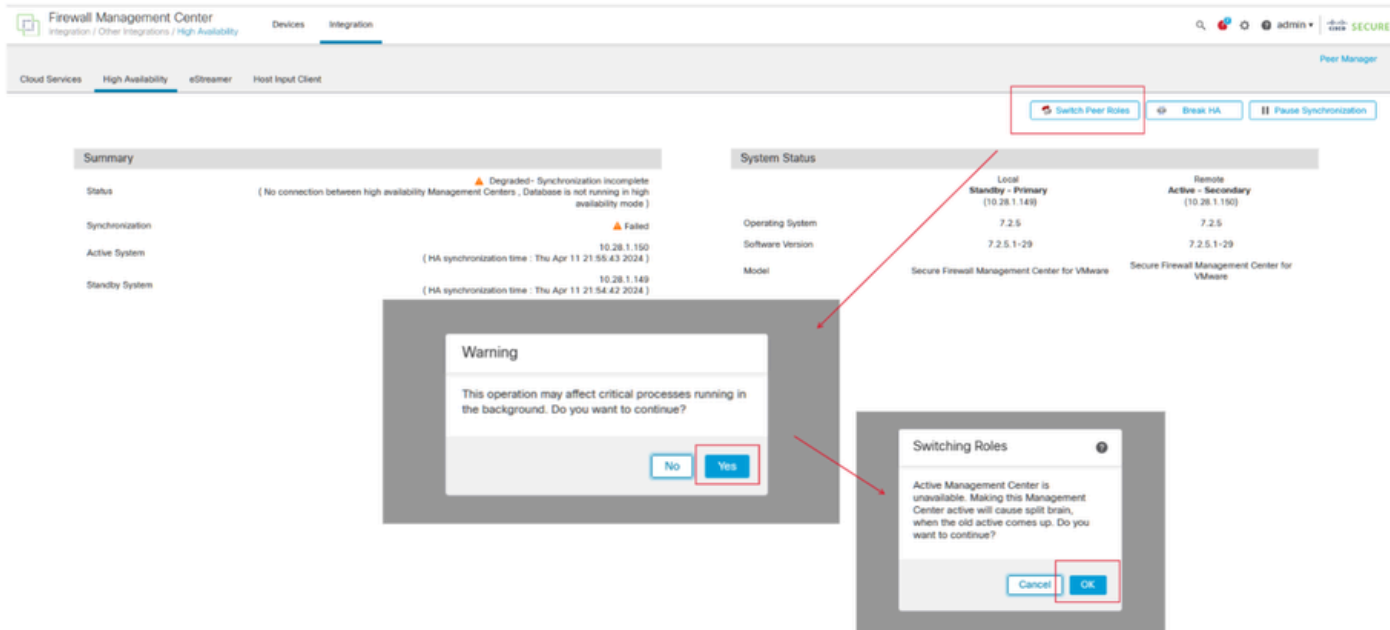
The 'Make Me Active' dialog box is open, asking: "Do you want to make this Management Center active and peer standby?". The 'OK' button is highlighted with a red box. A 'Warning' dialog box is also visible, stating: "This operation may affect critical processes running in the background. The local peer 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?". The 'Yes' button in the warning dialog is also highlighted with a red box.

Passaggio 7: Una volta completata la sincronizzazione, che può richiedere tempo, passare all'interfaccia Web dell'unità attiva. Modificare quindi i ruoli, posizionando la nuova unità come accessorio attivo.

Soluzione 2

Procedura per la sostituzione di un'unità difettosa senza backup

Passo 1: Assegnare l'unità operativa come attiva. Per ulteriori informazioni, fare riferimento a [Switching Peer in Management Center High Availability Pair.](#)



Passaggio 2: ricreare l'immagine della nuova unità in modo che corrisponda alla versione software dell'unità attiva. per ulteriori informazioni, fare riferimento a [Reimage a Hardware Model of a Cisco Secure Firewall Management Center](#) (Reimaging un modello hardware di un centro di gestione di Cisco Secure Firewall).

Passo 3: se necessario, aggiornare la stessa versione degli aggiornamenti del database di geolocalizzazione (GeoDB), degli aggiornamenti del database di vulnerabilità (VDB) e degli aggiornamenti software di sistema dell'unità attiva per garantire la coerenza.

Operational Unit

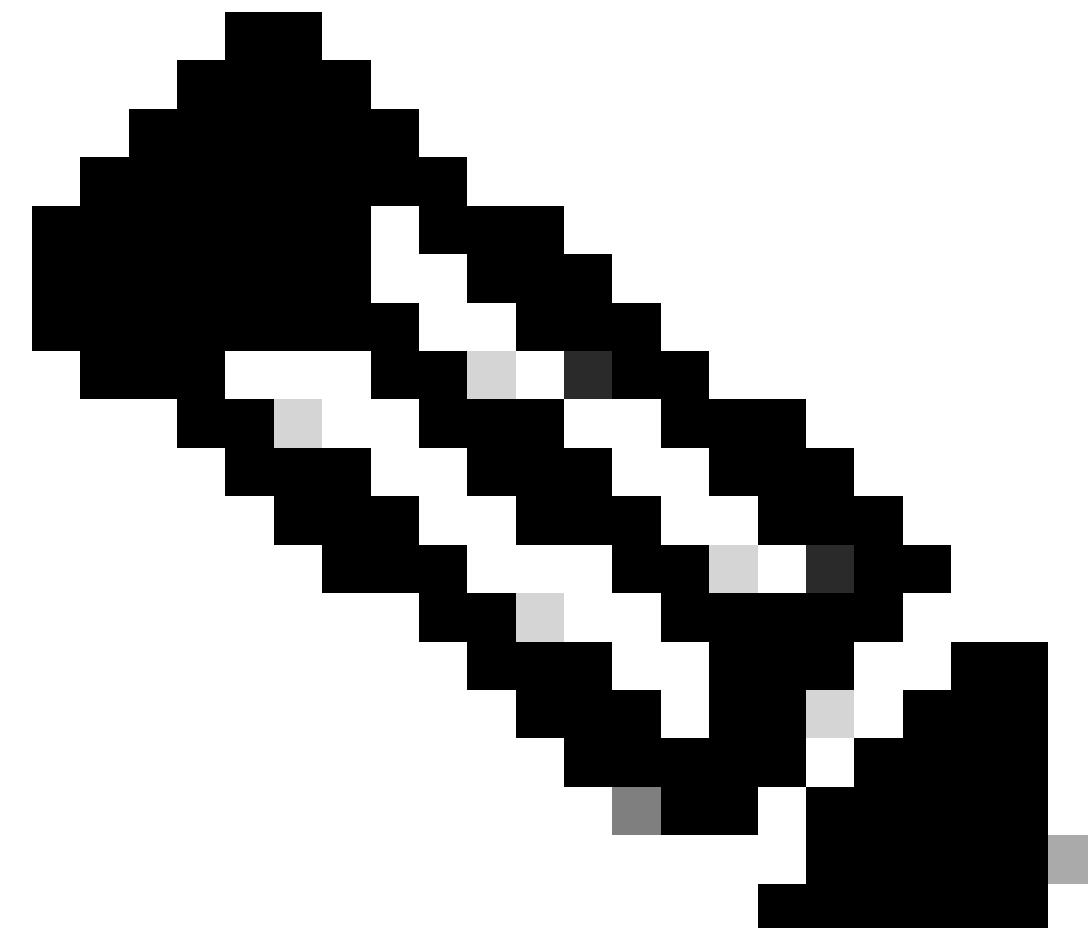
Replacement



Passaggio 4: utilizzare l'interfaccia Web del centro di gestione attivo per interrompere HA. Quando richiesto, selezionare l'opzione per gestire le periferiche registrate da questa console.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Integration' tab is active. Below the navigation bar, there are buttons for 'Switch Peer Roles', 'Break HA' (highlighted with a red box), and 'Pause Synchronization'. The main content area is divided into 'Summary' and 'System Status' sections. The 'Summary' section shows the status of the high availability configuration, including a warning for 'Degraded - Synchronization incomplete'. The 'System Status' section shows details for the local and remote systems, including their roles (Active-Primary and Standby-Secondary), operating systems, and software versions. A dialog box titled 'Break HA' is open, asking 'How do you want to manage devices after breaking high availability?' with three 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.

Fase 5: riconfigurare il centro di gestione HA configurando il centro di gestione operativo come principale e l'unità sostitutiva come secondaria. Per istruzioni dettagliate, vedere [Definizione della disponibilità elevata di Management Center](#).



Nota: quando si ristabilisce HA, la configurazione più recente del centro di gestione principale viene sincronizzata con quella del centro di gestione secondario. Le licenze

Classic e Smart sono progettate per integrarsi senza problemi.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Una volta completata la sincronizzazione, l'output previsto sarà Stato integro e Sincronizzazione OK.

The screenshot shows the Firewall Management Center (FMC) web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Integration' tab is selected. Below the navigation bar, there are several tabs: 'Cloud Services', 'Realms', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Manager On-Prem'. The 'High Availability' tab is active. The main content area is divided into two sections: 'Summary' and 'System Status'. The 'Summary' section shows a 'Status' of 'Healthy' (green dot) and a 'Synchronization' status of 'OK' (green dot). Below this, it lists 'Active System' and 'Standby System' with their respective IP addresses (10.28.1.149 and 10.28.1.150) and HA synchronization times. The 'System Status' section is a table with columns for 'Local' (Active - Primary) and 'Remote' (Standby - Secondary). It lists 'Operating System' (7.2.5), 'Software Version' (7.2.5.1-29), and 'Model' (Secure Firewall Management Center for VMware).

Poiché questo processo può richiedere del tempo, le unità primaria e secondaria sono ancora in fase di sincronizzazione. Durante questo periodo, verificare che i dispositivi siano elencati correttamente sia sull'unità principale che su quella secondaria.

Inoltre, è possibile eseguire la verifica tramite la CLI. A tale scopo, è necessario connettersi alla CLI, passare alla modalità Expert, elevare i privilegi ed eseguire questi script:

```
<#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

Per informazioni più dettagliate, vedere [Verificare la modalità Firepower, l'istanza, l'alta disponibilità e la configurazione della scalabilità.](#)

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Guida all'amministrazione di Cisco Secure Firewall Management Center, 7.4. Alta disponibilità](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).