Sostituzione di Secure Firewall Management Center in una coppia HA

Sommario

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

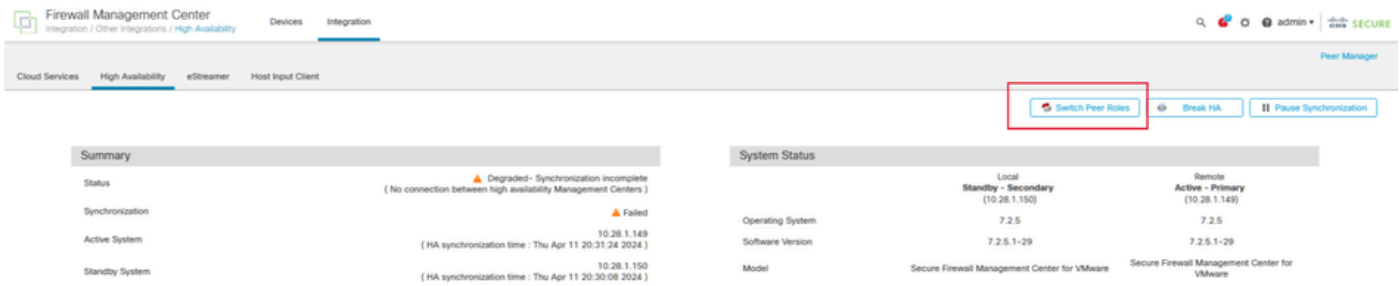
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

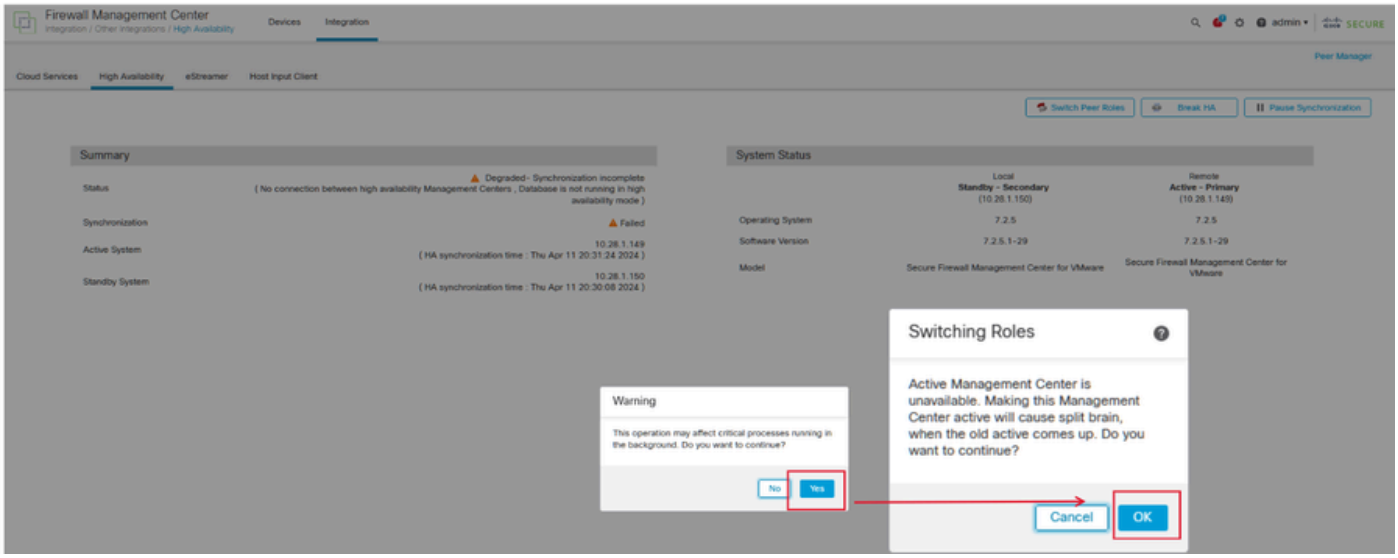
Configurazione

Soluzione 1

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

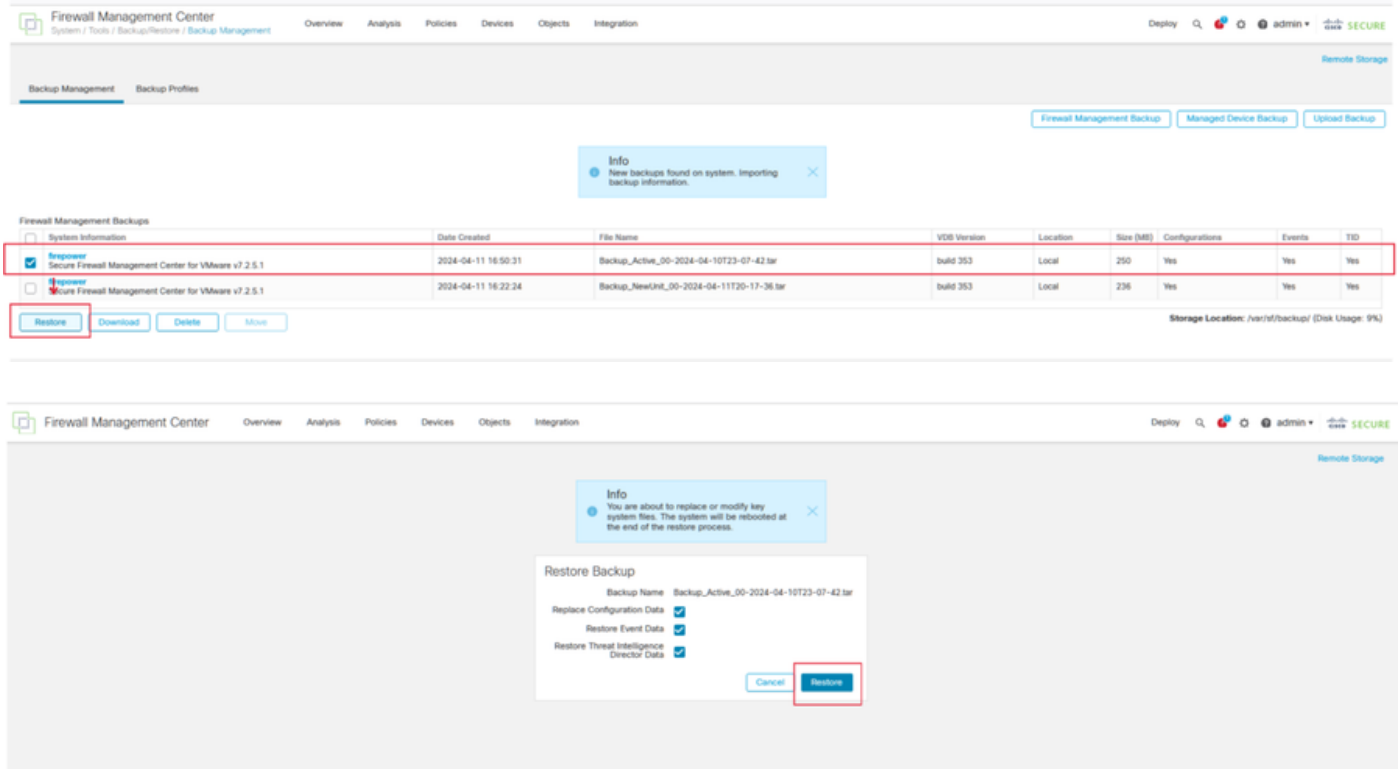
Passo 1: Assegnare l'unità operativa come attiva. Per ulteriori informazioni, fare riferimento a [Switching Peer in Management Center High Availability Pair.]





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.



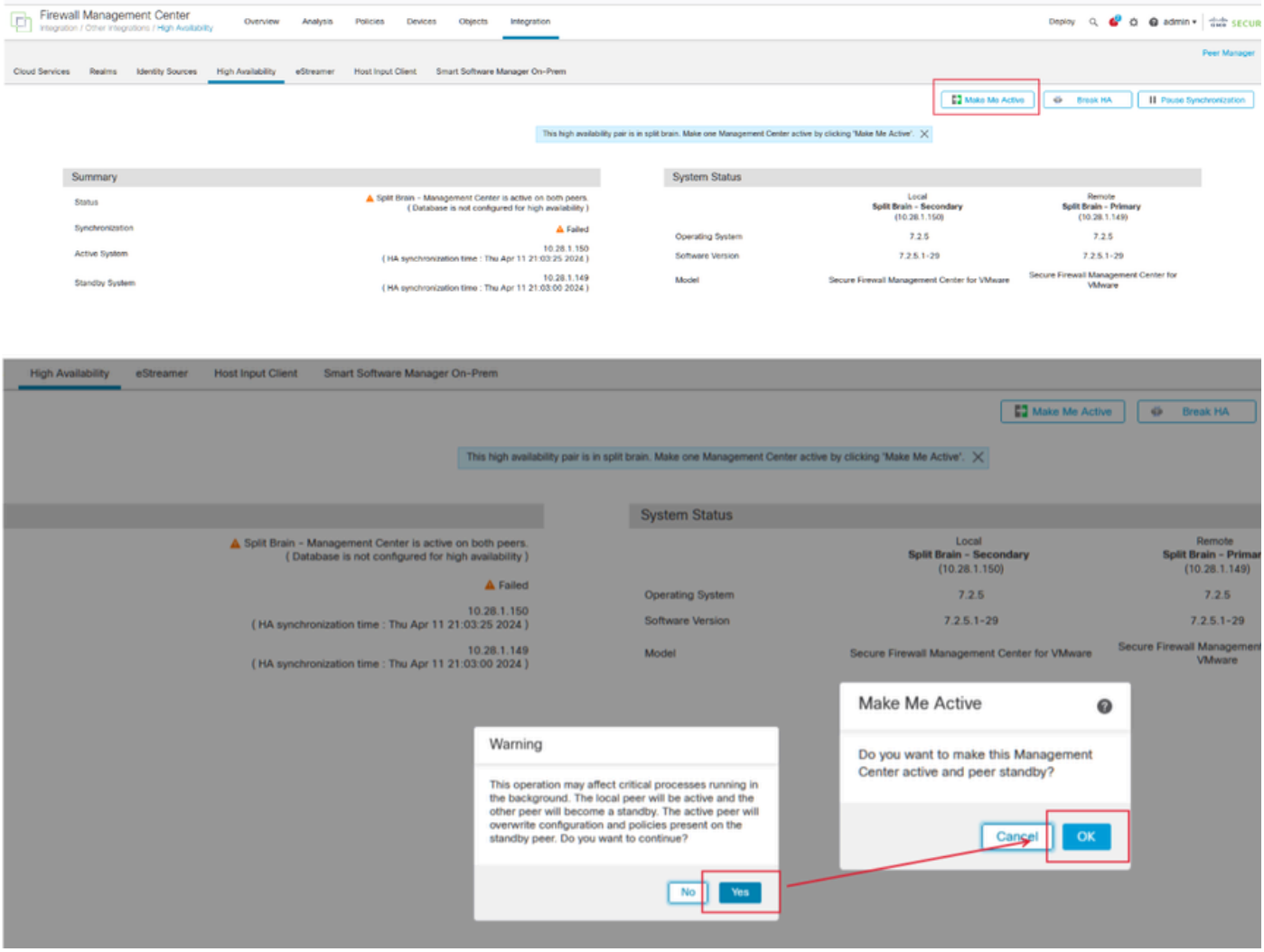
Passo 4: se necessario, aggiornare la stessa versione degli aggiornamenti del database di geolocalizzazione (GeoDB), degli aggiornamenti del database di vulnerabilità (VDB) e degli aggiornamenti software di sistema dell'unità attiva per garantire la coerenza.

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.

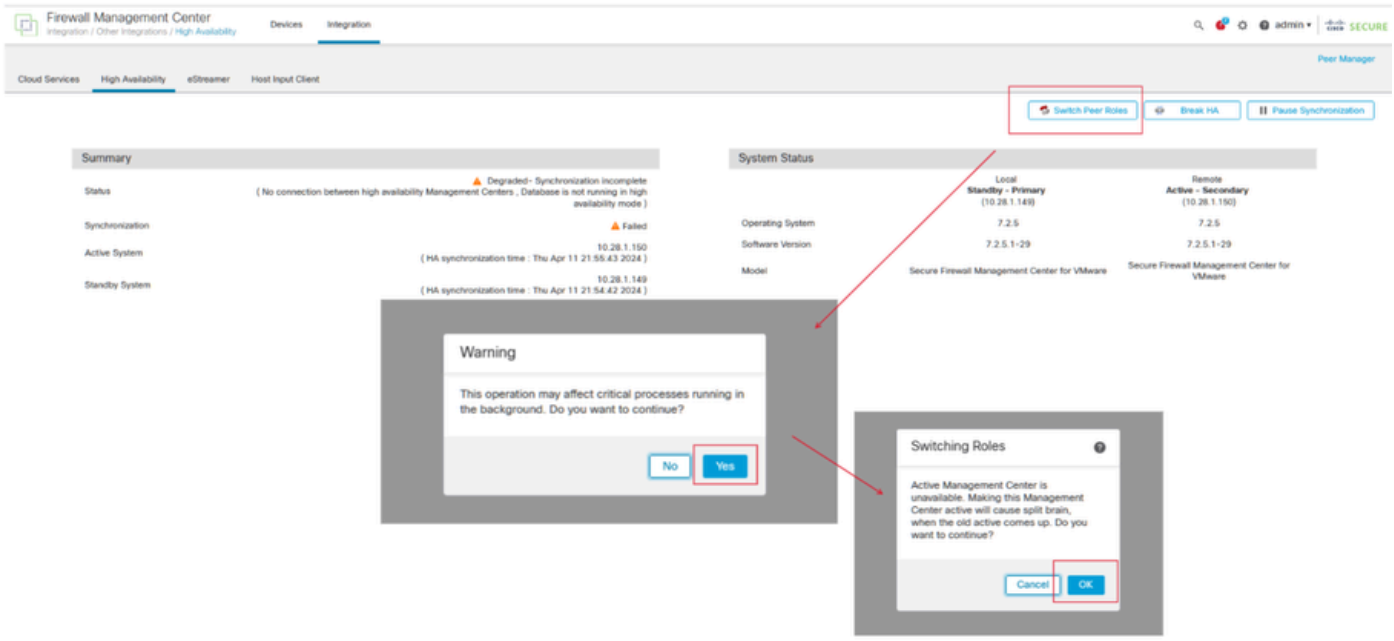


Passaggio 7: Una volta completata la sincronizzazione, che può richiedere tempo, passare all'interfaccia Web dell'unità attiva. Modificare quindi i ruoli, posizionando la nuova unità come accessorio attivo.

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.]



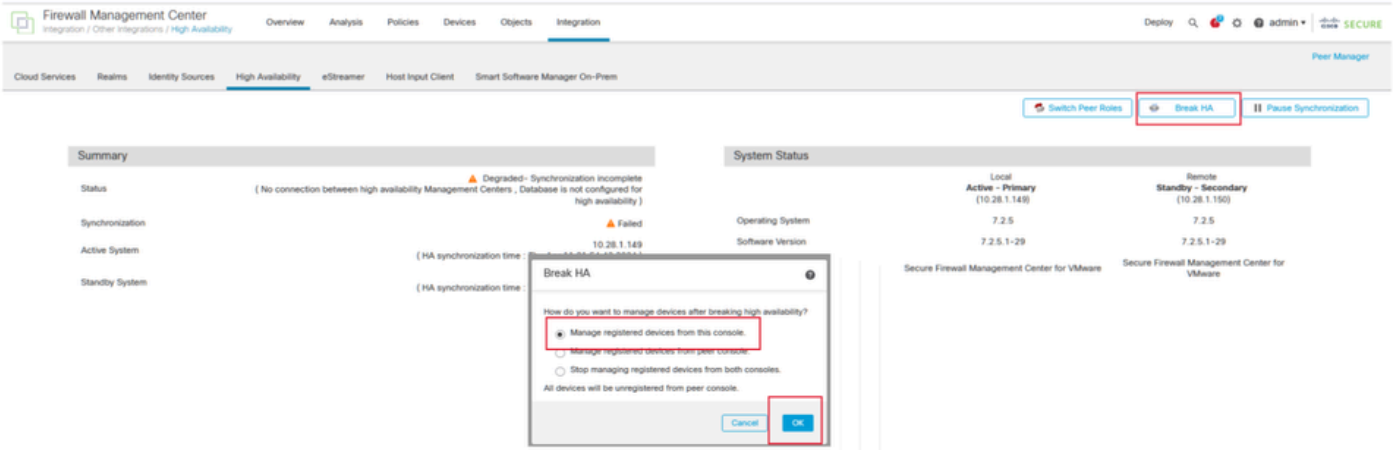
Passaggio 2: ricreare l'immagine della nuova unità in modo che corrisponda alla versione software dell'unità attiva. per ulteriori informazioni, fare riferimento a Reimage a Hardware Model of a Cisco Secure Firewall Management Center (Reimaging un modello hardware di un centro di gestione di Cisco Secure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

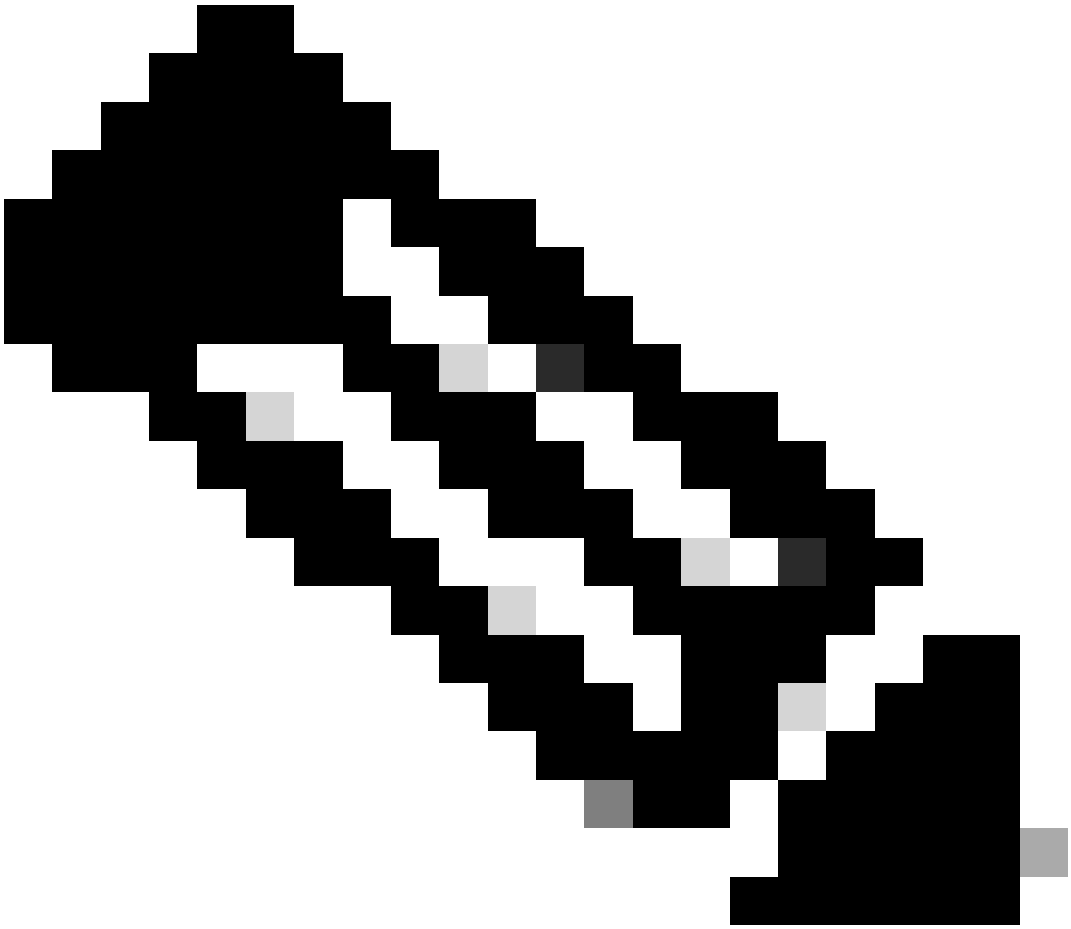
Operational Unit

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.



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.]



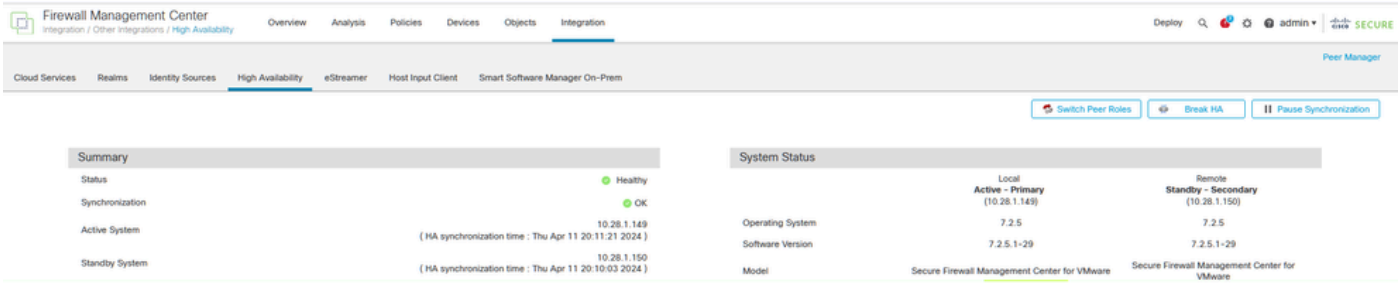
Nota: quando si ristabilisce HA, la configurazione più recente del centro di gestione principale viene sincronizzata con quella del centro di gestione secondario. Le licenze

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.



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).