Configurazione dell'alta disponibilità sui centri di difesa serie 3

Sommario

Introduzione

Questo documento descrive la configurazione di High Availability(HA) per i centri di difesa serie 3 (DC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Tecnologia Firepower
- Concetti di base dell'alta disponibilità

Componenti usati

Le informazioni fornite in questo documento si basano sui dispositivi Firepower Defense Center serie 3 (DC1500,DC2000,DC3500,DC4000) in esecuzione dalla versione software 5.3 alla versione software 5.4.1.6

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.

Premesse

Per garantire la continuità delle operazioni, la funzione di alta disponibilità consente di designare centri di difesa ridondanti per la gestione dei dispositivi.Il centro di difesa gestisce flussi di dati di eventi da dispositivi gestiti e determinati elementi di configurazione di tali dispositivi. Se un centro di difesa si guasta, è possibile monitorare la rete senza interruzioni tramite l'altro centro di difesa.

Caratteristiche di alta disponibilità

- La sincronizzazione HA è bidirezionale, il che significa che anche se esiste un dispositivo primario e secondario designato, le modifiche aggiunte su uno dei dispositivi vengono replicate sull'altro.
- HA non richiede la connessione diretta dei dispositivi. La connessione HA può essere effettuata su uno switch ma deve trovarsi nello stesso dominio di trasmissione.
- I dispositivi HA comunicano tramite l'IP di gestione alla porta 8305.
- Il tempo di sincronizzazione HA per un dispositivo è di cinque minuti, il che significa che dopo ogni cinque minuti un dispositivo tenta di sincronizzare la propria configurazione con il peer. Poiché il tempo necessario per la sincronizzazione è specifico dei dispositivi, cumulativamente il tempo di sincronizzazione può essere portato a dieci minuti.
- Se è necessaria una nuova immagine per un peer HA specifico, si consiglia di interrompere l'HA e quindi ricreare l'immagine.
- Se si intende aggiornare il cluster HA, non è necessario interrompere l'operazione. Quando si esegue l'aggiornamento dalla versione 5.3.0 alla 5.4.0, aggiornare i dispositivi uno alla volta e, una volta aggiornati, eseguire un'attività di sincronizzazione sul centro di difesa primario.
- La presenza di un criterio di accesso con lo stesso nome in entrambi i controller di dominio crea due criteri di controllo di accesso con lo stesso nome. Un criterio è configurato localmente e l'altro è sincronizzato dal controller di dominio peer.

  Nota: Impossibile aggiungere una destinazione o applicare il criterio perché genera un errore che indica che esiste già un criterio con lo stesso nome.
- Poiché le licenze non sono sincronizzate tra peer controller di dominio, è necessario aggiungerle separatamente ai controller di dominio.
- Tutti i dispositivi gestiti vengono aggiunti a un solo controller di dominio. La configurazione viene sincronizzata tra i controller di dominio peer.
- I dispositivi gestiti inviano registri a entrambi i controller di dominio.
- I controller di dominio sincronizzano le azioni più recenti. Ad esempio, se si elimina un utente da DC-1, l'altro controller di dominio peer non sincronizza la configurazione utente con DC-1. Sincronizza l'**azione di eliminazione** e l'utente viene perso sia da DC-1 che da DC-2.

Configurazione condivisa in modo bidirezionale tra peer

I controller di dominio HA sincronizzano i criteri in modo bidirezionale. Queste configurazioni vengono sincronizzate bidirezionalmente tra peer. È inoltre possibile visualizzare la maggior parte delle configurazioni con il percorso definito accanto:

Identità e autenticazione

- Configurazione LDAP esterno: passare a **Sistema > Locale > Gestione utenti > Autenticazione esterna**
- Utenti (interni ed esterni): passare **a Sistema > Locale> Gestione utenti> Utenti**
- Ruoli utente personalizzati: passare **a Sistema > Locale > Gestione utente > Ruoli utente**

Report

- Modelli di report: passare a **Panoramica > Report > Modelli di report**

Criteri Configurabili (Nella Sezione Criteri)

- Policy di controllo dell'accesso, policy sulle intrusioni, policy sui file, policy SSL, policy di accesso alla rete, policy e regole di correlazione, lista bianca di conformità e profili di traffico.
- Regole intrusione (locale e SRU): passare **a Criteri > Intrusione > Editor regole > Regole locali.**
- Individuazione della rete, attributi host, feedback degli utenti per l'individuazione della rete, incluse note e criticità dell'host, eliminazione di host, applicazioni e reti dalla mappa della rete e disattivazione o modifica delle vulnerabilità.
- Rilevatori di applicazioni personalizzati
- Connessioni LDAP nei criteri utente - Passare **a Criteri > Utenti**
- Avvisi: passare a **Criteri > Azioni > Avvisi** (sotto Risposte)

Informazioni dispositivo

- Regole NAT - Passare **a Dispositivi > NAT**
- Regole VPN: passare **a Dispositivi > VPN**
- Tutte le informazioni sul dispositivo, incluso il nome e il relativo gruppo, vengono sincronizzate in modo bidirezionale. Anche la posizione per l'archiviazione dei log di ciascun dispositivo viene sincronizzata tra peer - Selezionare **Dispositivi > Gestione dispositivi**
- Classificazioni regole intrusioni personalizzate
- Impronte digitali personalizzate attivate
- Criteri di sistema e criteri di integrità
- Dashboard personalizzati, flussi di lavoro personalizzati e tabelle personalizzate
- Modifica impostazioni riconciliazione, snapshot e report
- Aggiornamenti delle regole Sourcefire (SRU), aggiornamenti del database di geolocalizzazione (GeoDB) e aggiornamenti del database di vulnerabilità (VDB)

Configurazione non sincronizzata tra controller di dominio

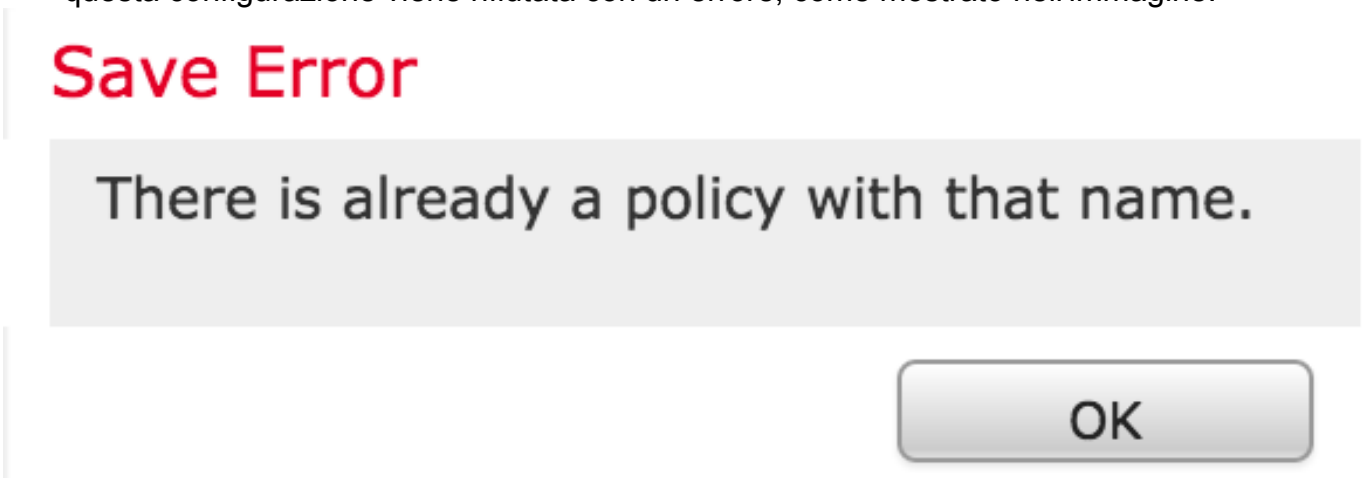
- Informazioni sull'agente utente nei criteri utente
- Scansioni NMAP
- Response Group
- Moduli di monitoraggio e aggiornamento

- Istanze di risoluzione
- Estreamer e host Input Client
- Profili di backup
- Programmazioni
- Licenze
- Aggiornamenti
- Avvisi sullo stato

Configurazione

Prerequisiti per la configurazione della disponibilità elevata

- I dispositivi devono essere della stessa versione software e hardware.
- È necessario che nei dispositivi sia installato lo stesso VDB.
- I dispositivi devono avere la stessa SRU.
- Assicurarsi che entrambi i centri difesa dispongano di un account utente denominato admin con privilegi di amministratore. Questi account devono utilizzare la stessa password.
- Accertarsi che i due Defense Center non dispongano di account utente con nomi identici a quelli dell'account admin. Rimuovere o rinominare uno degli account utente duplicati prima di stabilire la disponibilità elevata.
- Accertarsi che entrambe le periferiche non abbiano criteri di controllo dell'accesso con lo stesso nome. Se esistono due criteri di controllo di accesso con lo stesso nome, entrambi coesistono nei controller di dominio. Tuttavia, non possono essere associati ad alcun dispositivo.Dopo aver salvato il criterio dopo aver aggiunto un dispositivo di destinazione, questa configurazione viene rifiutata con un errore, come mostrato nell'immagine:



- Entrambi i centri di difesa devono avere accesso a Internet.

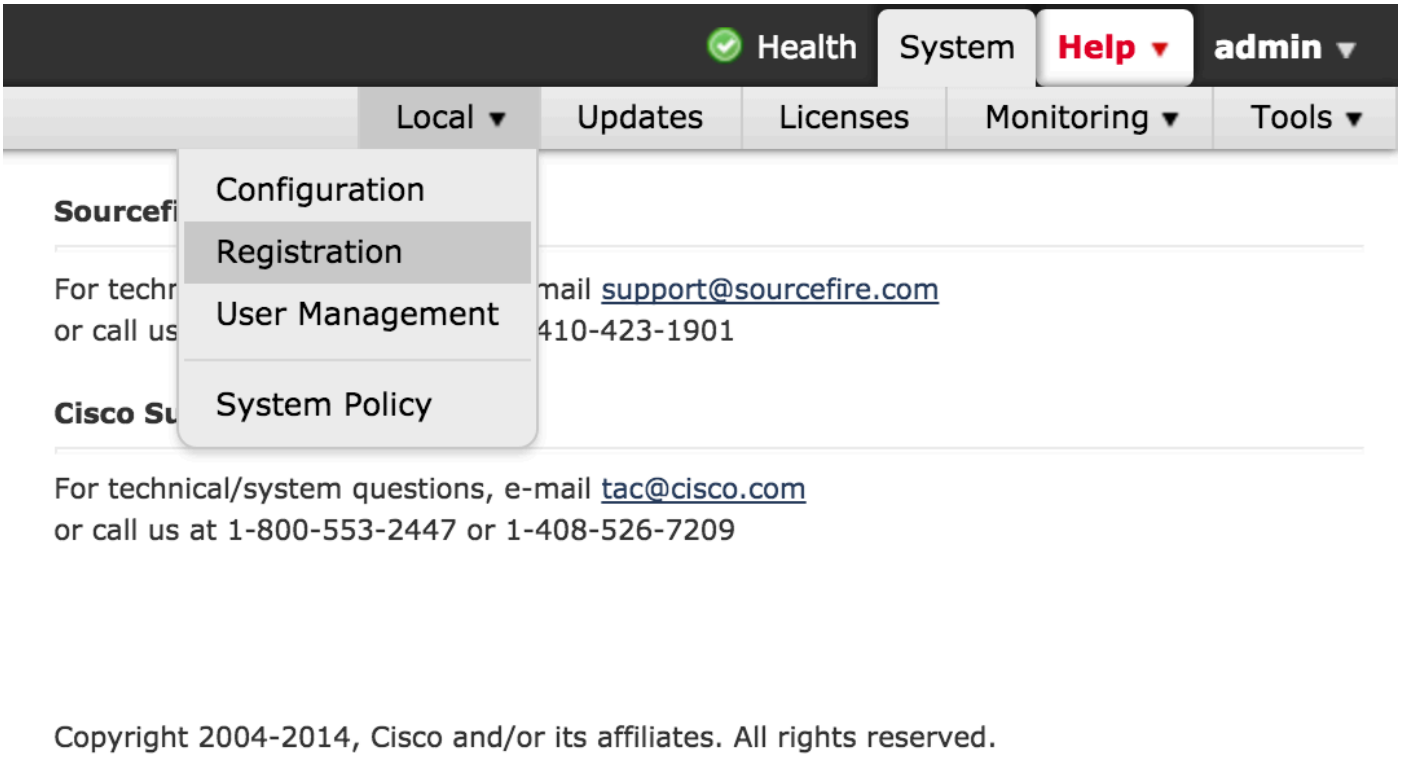
Configura alta disponibilità

Di seguito vengono illustrati gli 8 passaggi per configurare l'alta disponibilità.

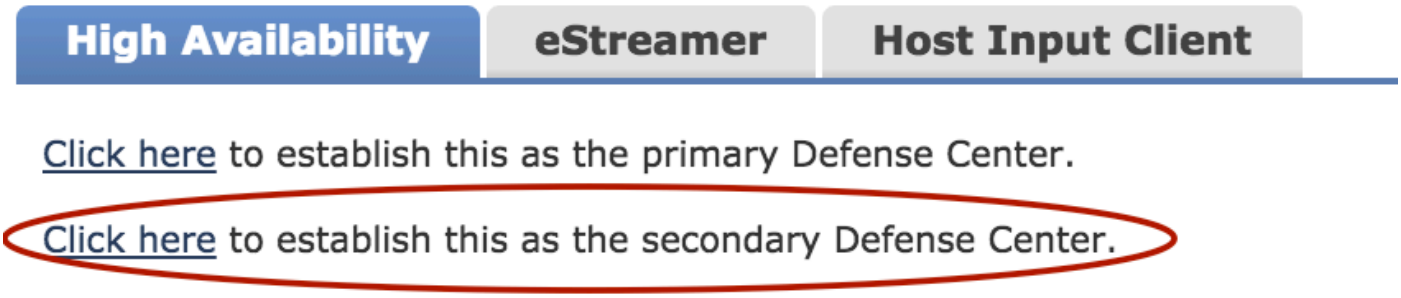
Passaggio 1. Verificare che la versione software e hardware, la versione VDB e la versione di aggiornamento della regola siano uguali.

Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build 258 (2015-11-10 22:58:57)

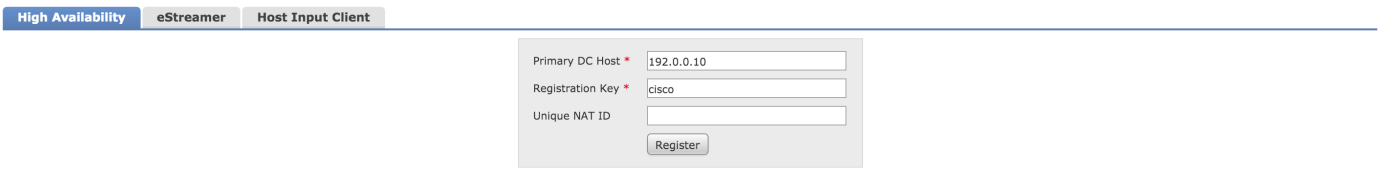
Passaggio 2. Per rendere il dispositivo secondario, selezionare **Sistema > Locale > Registrazione**, come mostrato nell'immagine. Verificare di non disporre di alcuna configurazione nel controller di dominio.



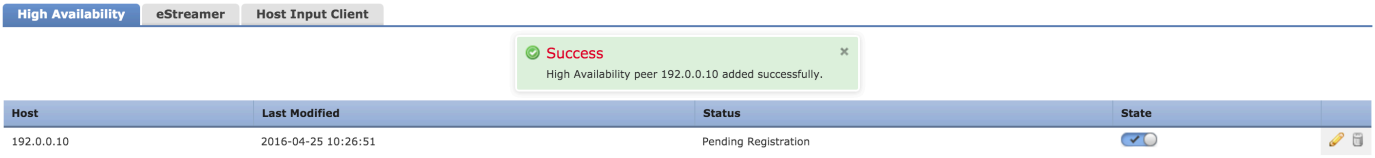
Passaggio 3. Sotto la scheda **Alta disponibilità** Fare clic su **Fare clic qui per impostare questo come centro di difesa secondario**, come mostrato nell'immagine:



Passaggio 4. Al termine del Passaggio 3, viene visualizzata una pagina come illustrato nell'immagine. Aggiungere l'indirizzo IP del controller di dominio primario e la passkey. Accertarsi di aggiungere un ID NAT univoco per i dispositivi dietro a Network Address Translation.



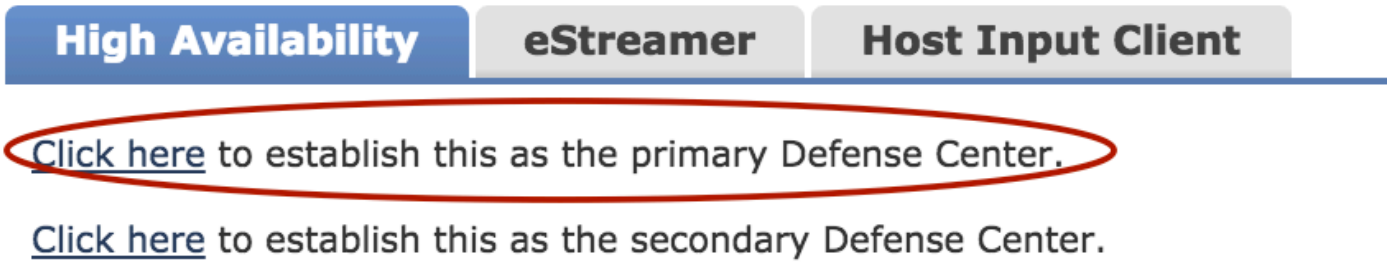
Passaggio 5. Dopo aver verificato l'indirizzo IP, fare clic su **Register** (Registra), se corretto. Viene visualizzata una pagina come illustrato nell'immagine:



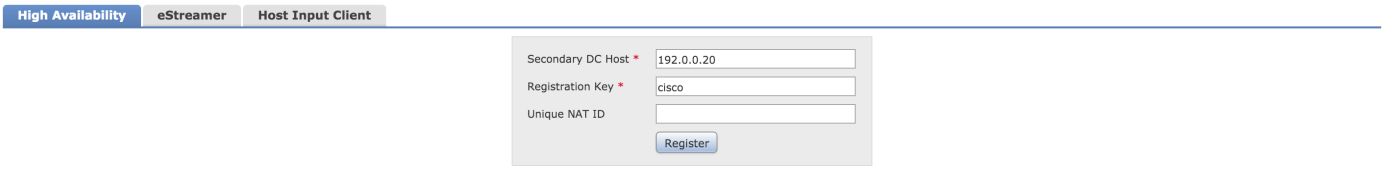
Ciò significa che HA è configurato sul controller di dominio secondario ed è necessario configurarlo sul controller di dominio primario.

Passaggio 6. Accedere al dispositivo che si desidera configurare come controller di dominio primario. Passare a **Sistema > Locale > Registrazione.**

Sotto la scheda **Alta disponibilità** Fare clic su **Fare clic qui per aggiungere come centro di difesa principale**, come mostrato nell'immagine:

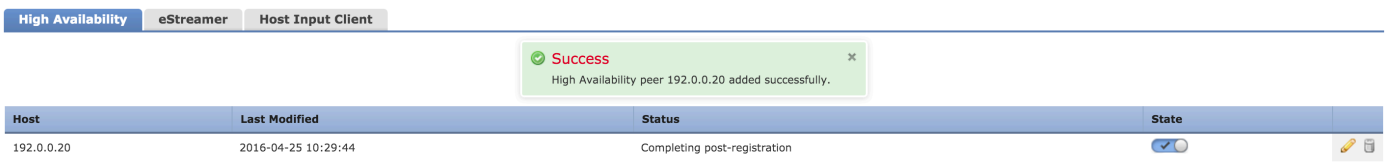


Passaggio 7. Dopo aver completato il Passaggio 6, viene visualizzata una pagina come illustrato nell'immagine:



Aggiungere l'indirizzo IP del controller di dominio secondario. Fornire la stessa chiave di registrazione e lo stesso ID NAT forniti durante la configurazione del controller di dominio secondario.

Passaggio 8. Dopo aver verificato i dettagli dell'indirizzo IP, fare clic su **Register.** Una volta completata la registrazione, viene visualizzata la pagina Successo come mostrato nell'immagine:



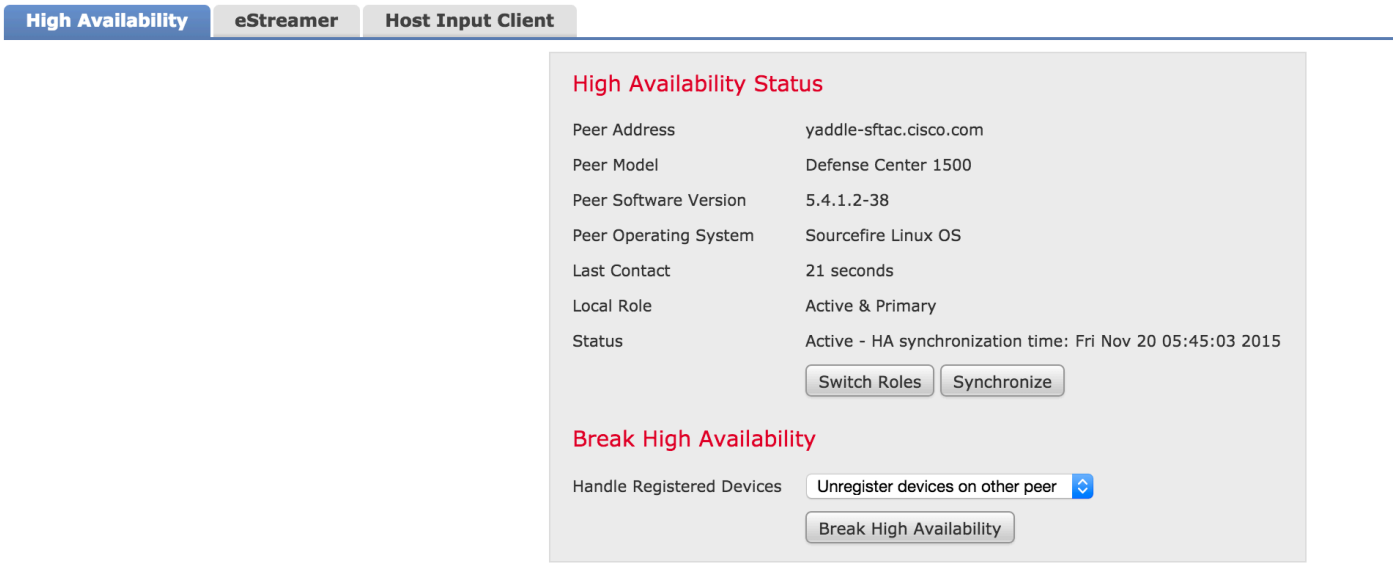
Dopo 5-10 minuti la configurazione e la sincronizzazione di HA sono completate.

Sono necessari circa 5-10 minuti per completare la configurazione e la sincronizzazione di HA

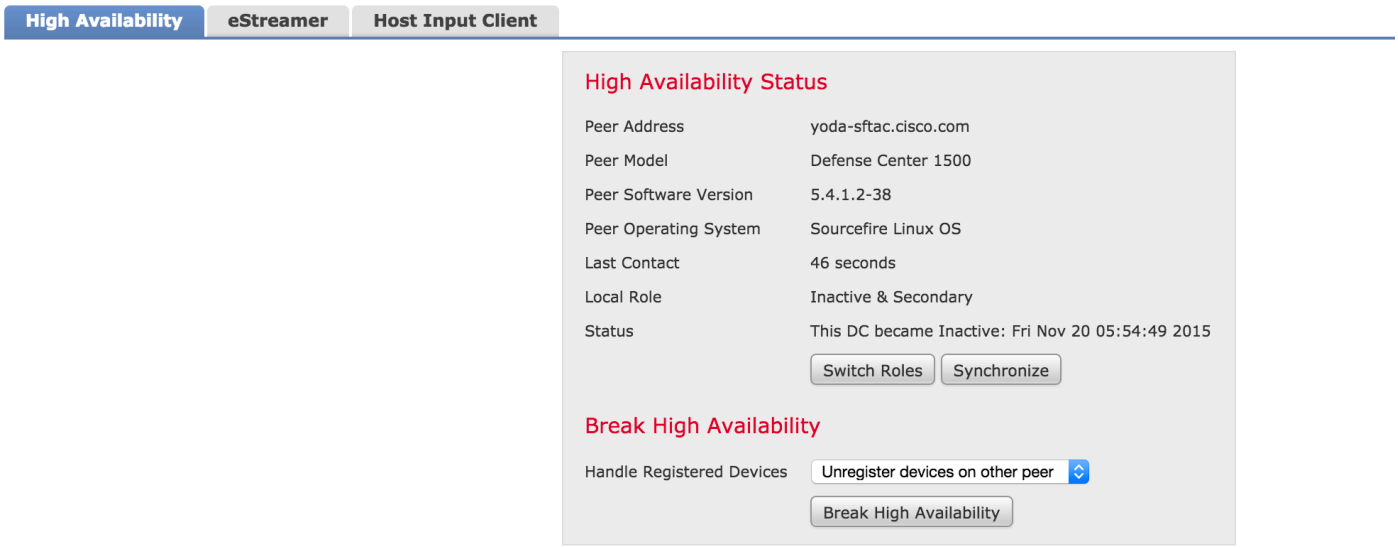
Verifica

Configurazione dettagliata per verificare che i controller di dominio siano configurati correttamente per la disponibilità elevata.

Passaggio 1. Passare a **System >Local >Registration** (Sistema > Locale > Registrazione) sul dispositivo principale, come mostrato nell'immagine:



Passaggio 2. Passare a **Sistema >Locale >Registrazione** sul dispositivo secondario come mostrato nell'immagine:



Risoluzione dei problemi

In questa sezione vengono illustrate le procedure di base per la risoluzione dei problemi di elevata

disponibilità.

- Assicurarsi che entrambi i controller di dominio siano in ascolto sulla porta TCP 8305, poiché HA utilizza questa porta per sincronizzare le informazioni e gli heartbeat.
- Verificare che la porta TCP 8305 non sia bloccata nella rete o da dispositivi intermedi.
- La creazione di HA non riesce se è presente una voce non aggiornata di un dispositivo peer precedente che viene rimossa o sostituita. La tabella EM_Peers fornisce ulteriori informazioni su tali dispositivi peer.

Informazioni correlate

- Configurazione dello stack sui dispositivi Cisco Firepower serie 8000
- Guida per l'utente di Firesight System 5.4.1
- Documentazione e supporto tecnico – Cisco Systems