Configuration de Haute disponibilité sur la gamme 3 centres de la défense

Contenu

Introduction

Ce document décrit la configuration de High Availability(HA) pour la défense Centers(DC) de la gamme 3.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologie de puissance de feu
- Concepts facilement disponibles de base

[Composants utilisés](#)

Les informations dans ce document sont basées sur la gamme de centre de la défense de puissance de feu 3 périphériques (DC1500,DC2000,DC3500,DC4000) exécutant de la version de logiciel 5.3 à la version de logiciel 5.4.1.6

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Pour assurer la continuité des exécutions, la caractéristique facilement disponible te permet pour indiquer les centres redondants de la défense pour gérer des périphériques. Le centre de la défense met à jour les flux de données d'événement des périphériques gérés et de certains éléments de configuration de ces périphériques. Si l'une défense centrale échoue, vous pouvez surveiller votre réseau sans interruption par l'autre centre de la défense.

Caractéristiques facilement disponibles

- L'ha de synchronisation est bidirectionnel qui signifie quoiqu'il y ait un périphérique primaire et secondaire indiqué, des modifications ajoutées sur des n'importe quels des périphériques est répliquée vers l'autre.

- L'ha n'exige pas des périphériques d'être directement connectés. La connexion ha peut être faite au-dessus d'un commutateur mais cette connexion doit être dans le même domaine d'émission.

- Les périphériques ha communiquent au-dessus de leur IP de Gestion au port 8305.

- L'ha de temps de synchronisation pour un périphérique est de cinq minutes, ainsi il signifie qu'après que chaque cinq minute des tentatives d'un périphérique de synchroniser sa configuration avec son pair. Puisque la durée requise pour la synchronisation est spécifique aux périphériques, cumulativement, le temps de synchronisation peut être maximisé à dix minutes.

- Si un réimager est exigé pour un pair ha de particularité il est recommandé de casser l'ha et puis de réimager.

- Si vous prévoyez d'améliorer la batterie ha il n'est pas nécessaire de casser l'ha. Quand vous améliorez des versions 5.3.0 à 5.4.0, améliorez les périphériques un et une fois qu'ils sont améliorés effectuez une tâche de synchronisation au centre de défense principale.

- La présence d'une stratégie d'accès avec le même nom sur chacun des deux DCS créent deux stratégies de contrôle d'accès du même nom. Une stratégie est configurée localement et l'autre est synchronisée du C.C de pair.

  Remarque: Vous ne pouvez pas ajouter une cible ou appliquer cette stratégie parce qu'elle jette une erreur, qui déclare qu'il y a déjà une stratégie avec le même nom.

- Des permis ne sont pas synchronisés entre les pairs C.C, donc, ils sont exigés pour être ajoutés séparément à DCS.

- Tous les périphériques gérés sont ajoutés seulement à un C.C. La configuration est synchronisée entre DCS de pair.

- Les périphériques gérés envoient à des logs à chacun des deux DCS.

- DCS synchronisent les dernières actions. Par exemple, si vous supprimez un utilisateur de DC-1, l'autre pair DC-2 ne synchronise pas la configuration utilisateur à DC-1. Il synchronise l'**action d'effacement** et l'utilisateur est perdu de DC-1 et de DC-2.

Configuration partagée bidirectionnel entre les pairs

L'ha DCS synchronise des stratégies bidirectionnel. Ces configurations synced bidirectionnel entre les pairs. Vous pouvez également visualiser la plupart de ces configurations avec le chemin défini juste à côté de lui :

Identités et authentification

- La configuration externe de LDAP naviguent vers le **système > les gens du pays > la gestion des utilisateurs > l'authentification externe**
- Utilisateurs (interne et externe) - Naviguez le toSystem **> les utilisateurs de Management> d'utilisateur de Local>**
- Les rôles d'utilisateur faits sur commande naviguent le toSystem **> les gens du pays > la gestion des utilisateurs > les rôles de l'utilisateur**

États

- Les descripteurs d'état naviguent vers l'**aperçu > l'enregistrement > les modèles de rapport**

Stratégies configurables (sous la section de stratégies)

- Stratégies de contrôle d'accès, stratégies d'intrusion, stratégies de fichier, stratégies de stratégies SSL, d'accès au réseau, stratégies et règles de corrélation, whitelist de conformité et profils du trafic.
- Des règles d'intrusion (des gens du pays et SRU) - naviguez les toPolicies **> l'éditeur de règle d'Intrusion> > des règles locales.**
- Détection de réseau, attributs d'hôte, feedback des utilisateurs de détection de réseau, y compris des notes et la criticité d'hôte, la suppression des hôtes, des applications, et des réseaux de la carte du réseau et la mise hors fonction ou la modification des vulnérabilités.
- Détecteurs d'application personnalisée
- Les connexions de LDAP dans des politiques d'utilisateur naviguent des toPolicies **> des utilisateurs**
- Les alertes naviguent vers des **actions > des alertes de Policies>** (sous des réponses)

L'information sur le périphérique

- Les règles NAT naviguent des toDevices **> NAT**
- Les règles VPN naviguent des toDevices **> le VPN**
- Toute l'information sur le périphérique comprenant le nom et son groupe synced bidirectionnel. L'emplacement pour la mémoire de log pour chaque périphérique synced également entre les pairs - naviguez les toDevices **> la Gestion de périphériques**
- Classifications faites sur commande de règle d'intrusion
- Empreintes digital faites sur commande lancées
- Stratégie de système et politique sanitaire
- Tableaux de bord faits sur commande, processus faits sur commande et tables faites sur commande
- Réconciliation, instantanés et paramètres de rapport de modification

- Base de données des mises à jour (SRU), du Geolocation de règle de Sourcefire (GeoDB), et mises à jour de la base de données de vulnérabilité (VDB)

Configuration synced entre DCS

- Les informations sur un agent d'utilisateur dans la stratégie d'utilisateur
- Balayages NMAP
- Groupes de réponse
- Modules de correction
- Exemples de correction
- Estreamer et client d'entrée d'hôte
- Profils de sauvegarde
- Programmes
- Permis
- Mises à jour
- Alertes de santés

Configurez

Conditions préalables pour configurer la Haute disponibilité

- Les périphériques doivent être du mêmes logiciel et version de matériel.

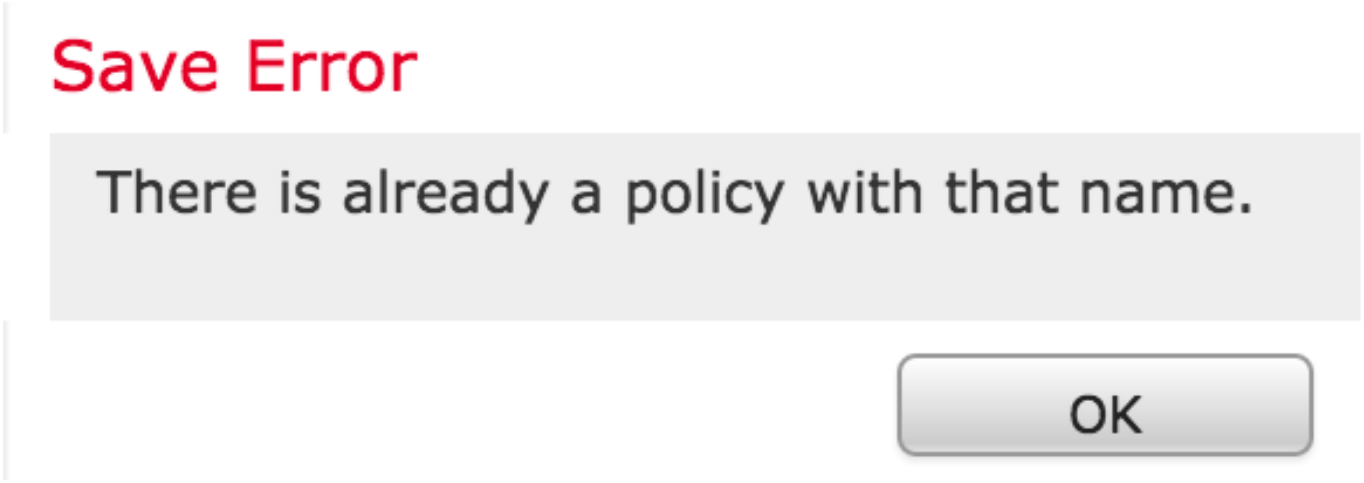
- Les périphériques doivent avoir le même VDB installé.

- Les périphériques doivent avoir le même SRU.

- Assurez que les deux centres de la défense ont un compte utilisateur nommé admin avec des privilèges d'administrateur. Ces comptes doivent utiliser le même mot de passe.

- Assurez-vous qu'autre que le compte d'admin, les deux centres de la défense n'ont pas des comptes utilisateurs avec des noms d'utilisateur identiques. Retirez ou renommez un du compte d'utilisateurs en double avant que vous établissiez la Haute disponibilité.

- Assurez que les les deux les périphériques n'ont aucune stratégie de contrôle d'accès avec le même nom. S'il y a deux stratégies de contrôle d'accès avec le même nom ils chacun des deux coexistent sur DCS. Cependant, ils ne peuvent pas obtenir associé à aucun périphérique. Une fois que vous sauvegardez cette stratégie après avoir ajouté un périphérique cible, cette configuration est rejetée avec une erreur suivant les indications de l'image :



- Les les deux les centres de la défense doivent avoir accès à l'Internet.

Configurez la Haute disponibilité

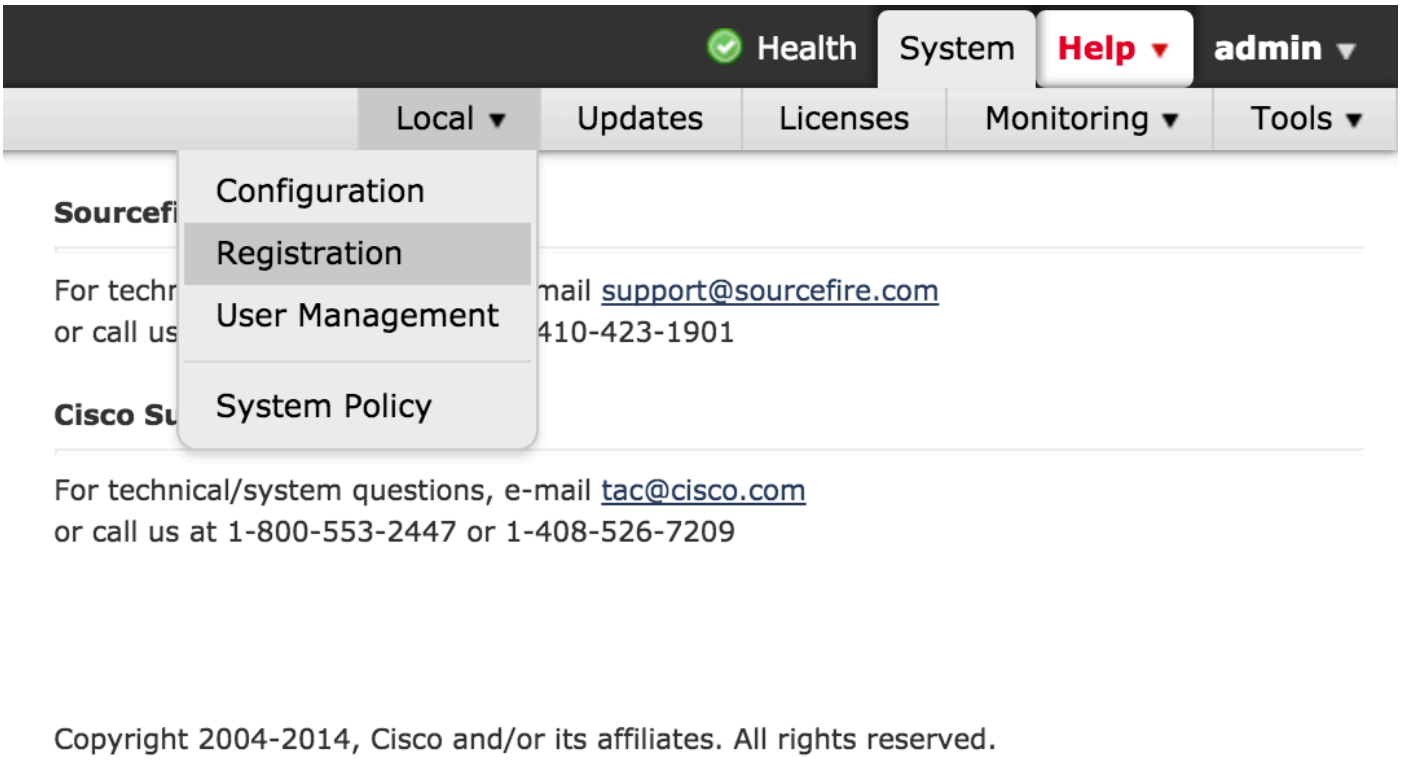
Ce sont les 8 étapes pour configurer la Haute disponibilité.

Étape 1. Confirmez que le logiciel et la version de matériel avec la version VDB et la version de mise à jour de règle sont identique.

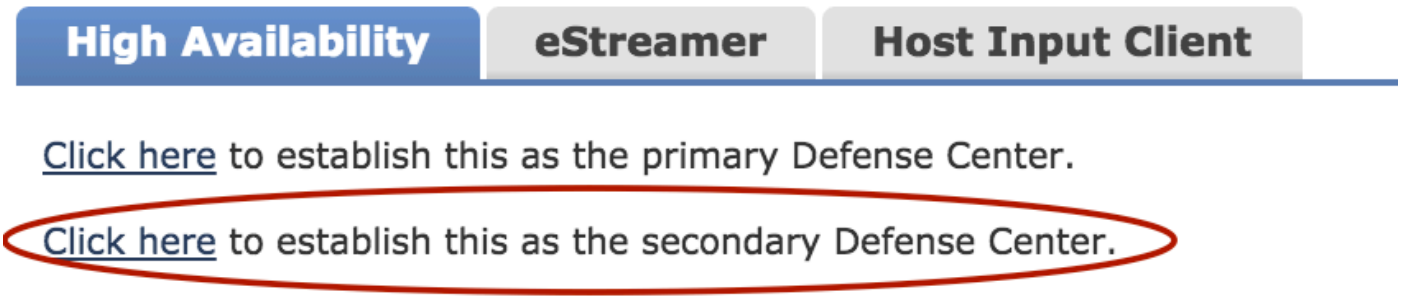
Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build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

Étape 2. Afin de rendre votre périphérique secondaire, naviguez vers le **système > les gens du pays > l'enregistrement**, suivant les indications de l'image. Assurez-vous que vous n'avez aucune

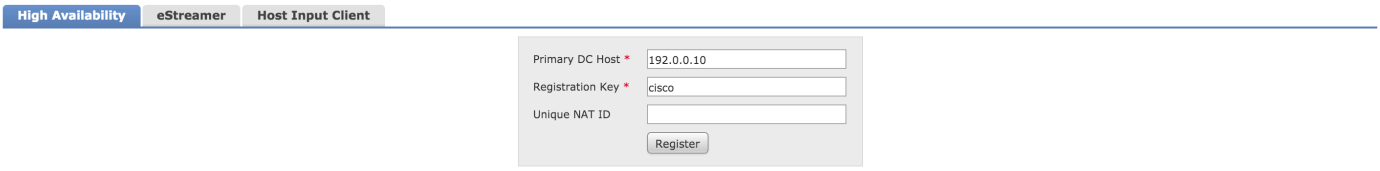
configuration sur ce C.C.



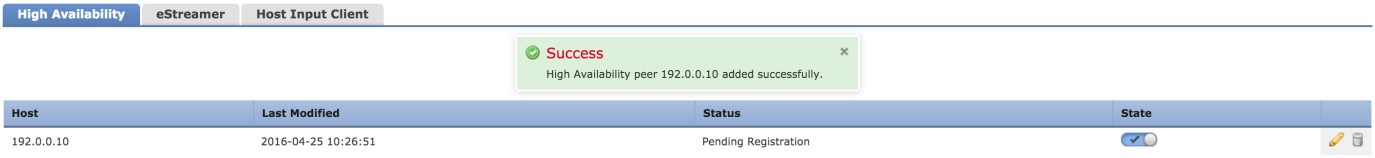
Étape 3. Sous l'onglet **facilement disponible** cliquez sur en fonction **Click here pour établir ceci comme centre secondaire de la défense**, suivant les indications de l'image :



Étape 4. Car vous vous terminez l'étape 3, une page est affichée suivant les indications de l'image. Ajoutez l'IP du C.C primaire et de la clé de passage. Assurez-vous que vous ajoutez un seul ID NAT pour les périphériques, qui sont derrière une traduction d'adresses réseau.



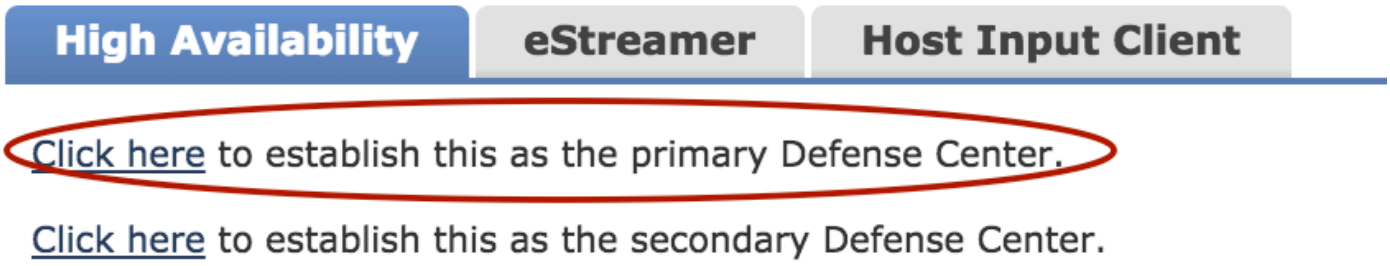
Étape 5. Après que l'adresse IP soit vérifiée, si correct cliquez sur en fonction le **registre**. Vous voyez une page suivant les indications de l'image :



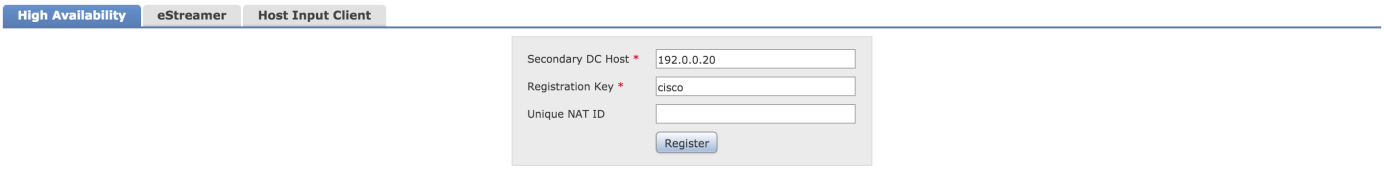
Ceci signifie que l'ha est configuré sur le C.C secondaire et vous doit le configurer sur le C.C primaire.

Étape 6. Procédure de connexion au périphérique que vous souhaitez configurer comme C.C primaire. Naviguez vers le **système > les gens du pays > l'enregistrement.**

Sous l'onglet **facilement disponible** cliquez sur en fonction **Click here pour ajouter comme centre de défense principale**, suivant les indications de l'image :

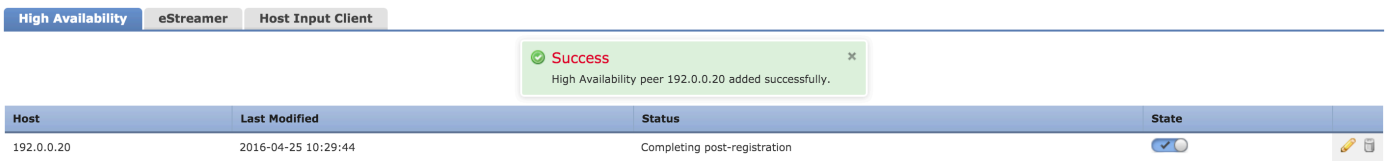


Étape 7. Après que vous vous terminiez l'étape 6, une page est affichée suivant les indications de l'image :



Ajoutez l'IP C.C secondaire. Fournissez la mêmes clé d'enregistrement et id NAT qui a été fourni tandis que vous configuriez le C.C secondaire.

Étape 8. Après que les détails de l'IP soient vérifiés cliquez sur en fonction le **registre.** Une fois que l'enregistrement est complet, la page de succès est vue suivant les indications de l'image :



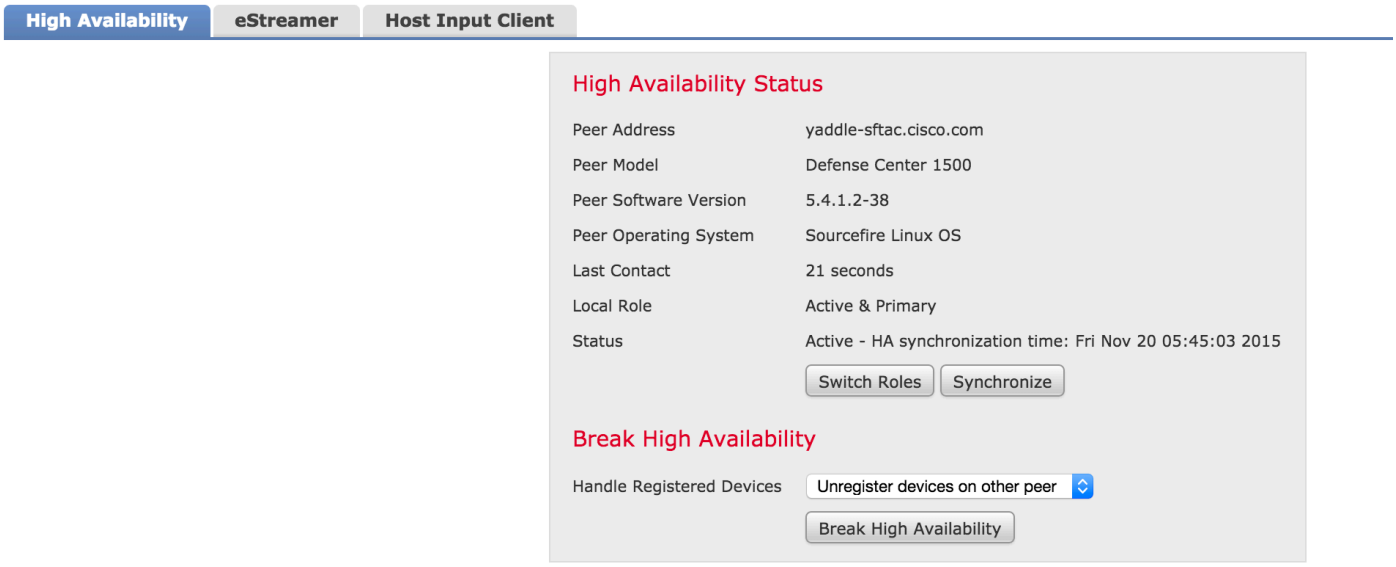
Après les minutes 5-10 la configuration et la synchronisation de l'ha sont terminées.

Cela prend presque 5-10 minutes afin de se terminer la configuration et la synchronisation de l'ha

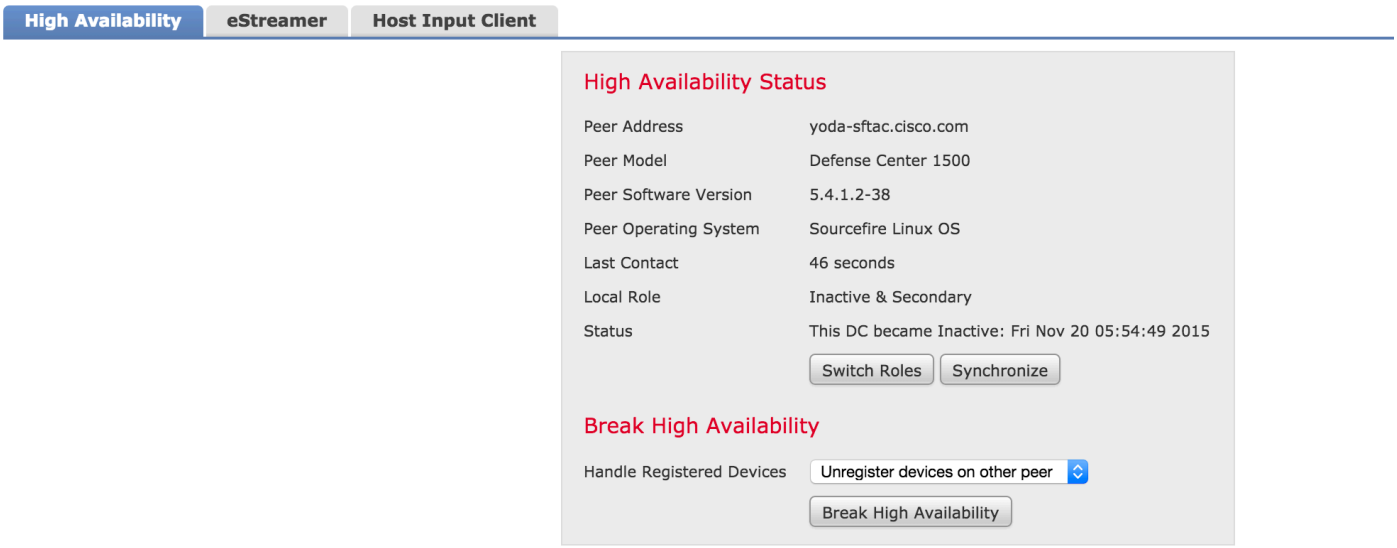
Vérifiez

Configuration pas à pas à vérifier que vos C.C sont configurés correctement pour la Haute disponibilité.

Étape 1. Naviguez vers le **>Registration >Local de système** sur le périphérique maître suivant les indications de l'image :



Étape 2. Naviguez vers le **>Registration >Local de système** sur le périphérique secondaire suivant les indications de l'image :



Dépannez

Cette section fournit les étapes de dépannage de base pour la Haute disponibilité.

- Assurez que chacun des deux les C.C écoutent sur le port TCP 8305, puisque l'ha emploie ce port pour synchroniser les informations et des pulsations.
- Assurez que le port TCP 8305 n'est bloqué dans le réseau ou par aucun périphérique intermédiaire.
- La création ha échoue s'il y a une entrée éventée d'un périphérique précédent de pair qui est retiré ou remplacé. La table d'EM_Peers fournit plus d'informations sur de tels périphériques de pair.

Informations connexes

- Configuration de pile sur les périphériques de gamme 8000 de puissance de feu de Cisco
- Guide utilisateur 5.4.1 de système de Firesight
- Support et documentation techniques - Cisco Systems