シリーズ 3 Defense Center での高可用性の設定

目次

概要

この資料はシリーズ 3 防御 Centers（DC）のための High Availability（HA）の設定を説明したものです。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower テクノロジー
- 基本的な高可用性の概念

使用するコンポーネント

この文書に記載されている情報は Firepower 防衛センター シリーズにソフトウェア バージョン 5.3 からソフトウェア バージョンから 5.4.1.6 を実行する 3 つのデバイス（DC1500,DC2000,DC3500,DC4000）基づいています

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

オペレーションの継続を確認するために、高可用性の機能はデバイスを管理するために冗長 な防御センターを指定することを可能にします。防御センターはこれらのデバイスの管理対象装置およびある特定の設定要素からのイベントデータ ストリームを維持します。 センター 1 つの防御が失敗した場合、他の防御センターによって割り込みなしでネットワークを監視できます。

高可用性の機能

- HA 同期は指定プライマリおよびセカンダリデバイスがあるのに双方向です、デバイスのどれでもで追加される変更複製される意味する他に。
- HA はデバイスが直接接続されるように要求しません。 HA 接続はスイッチにすることができますが、この接続は同じブロードキャスト ドメインにある必要があります。
- HA デバイスはポート 8305 で管理 IP に交信を行います。
- デバイスのための HA 同期 時間は 5 分です、つまり 5 分毎にデバイスがピアと設定を同期するように試みた後ことを意味します。 同期に必要な時間以来デバイスに特定、累積によって、10 分に同期 時間が最大化することができますです。
- イメージ変更が仕様 HA ピアに必要となれば HA を壊し、次にイメージ変更することを推奨します。
- HA クラスタをアップグレードすることを計画すれば HA を壊すことは必要ではないです。バージョン 5.3.0 から 5.4.0 へアップグレードするとき、デバイスを一つずつアップグレードし、アップグレードされたらプライマリ防衛 センターの同期 タスクを行って下さい。
- 両方の DC の同じ名前のアクセスポリシーの存在は同じ名前の 2 つのアクセスコントロールポリシーを作成します。 1 ポリシーはローカルで設定され、他はピア DC から同期されます。

  注: 既に同じ名前のポリシーがあっていることを示す工ラーを投げるのでターゲットを追加するか、またはこのポリシーを適用できません。
- ライセンスは DC 同位の間で同期されません、従って、DC に別々に追加されるために必要となります。
- すべての管理対象装置は 1 DC にだけ追加されます。 設定はピア DC の間で同期されます。
- 管理対象装置は両方の DC に口グを送信 します。
- DC は最新の操作を同期します。 たとえば、DC-1 からユーザを削除すれば、他のピア DC-2 は DC-1 にユーザコンフィギュレーションを同期しません。 それは**削除操作を**同期し、ユーザは DC-1 及び DC-2 両方から失われます。

同位の間で双方向に共有される設定

HA DC はポリシーを双方向に同期します。 これらのコンフィギュレーションは同位の間で双方向に同期されます。 またそれの隣でパスによって定義される権限のこれらのコンフィギュレーションのほとんどを表示できます:

識別および認証

- **システム > ローカル > ユーザマネージメント > 外部認証**への外部 LDAP 設定ナビゲート
- ユーザ（内部および外部）-ナビゲート toSystem **> Local> ユーザ Management> ユーザ**
- カスタム ユーザの役割ナビゲート toSystem **> ローカル > ユーザマネージメント > ユーザの役割**

レポート

- **外観**へのレポート テンプレート ナビゲート **> > レポート テンプレートを報告します**

設定可能なポリシー（ポリシー セクションの下で）

- アクセスコントロール ポリシー、不正侵入ポリシー、ファイル ポリシー、SSL ポリシー、ネットワーク アクセス ポリシー、相関ポリシーおよびルール、準拠性 whitelist およびトラフィックプロファイル。
- 不正侵入ルール（ローカルおよび SRU）-ナビゲート toPolicies **> Intrusion> ルール エディタ > ローカル ルール。**
- ネットワーク開発、ホスト属性、ホストのメモおよびホスト緊急度、削除、脆弱性のネットワークマップからのアプリケーションおよびネットワークを含むネットワーク開発 ユーザ フィードバック、および非アクティブ化または修正。
- カスタム アプリケーション探知器
- ユーザ ポリシー ナビゲート toPolicies **> Users** の LDAP 接続
- **Policies> 操作 > アラート**へのアラート ナビゲート（応答の下で）

デバイス情報

- NAT ルール ナビゲート toDevices **> NAT**
- VPN ルール ナビゲート toDevices **> VPN**
- 名前およびグループを含むすべてのデバイス情報は双方向に同期されます。 各デバイスの口グ ストレージのための Location はまた同位の間で-ナビゲート toDevices **> デバイス管理**同期されます
- カスタム不正侵入ルール分類
- アクティブにされたカスタム フィンガープリント
- システム ポリシーおよび健康政策
- カスタム ダッシュボード、カスタム作業の流れおよびカスタム表
- 和解、スナップショットおよびレポート設定を変更して下さい
- Sourcefire は更新（SRU）、Geolocation データベース（GeoDB）、および脆弱性データベース（VDB）更新を支配します

DC の間で同期されない設定

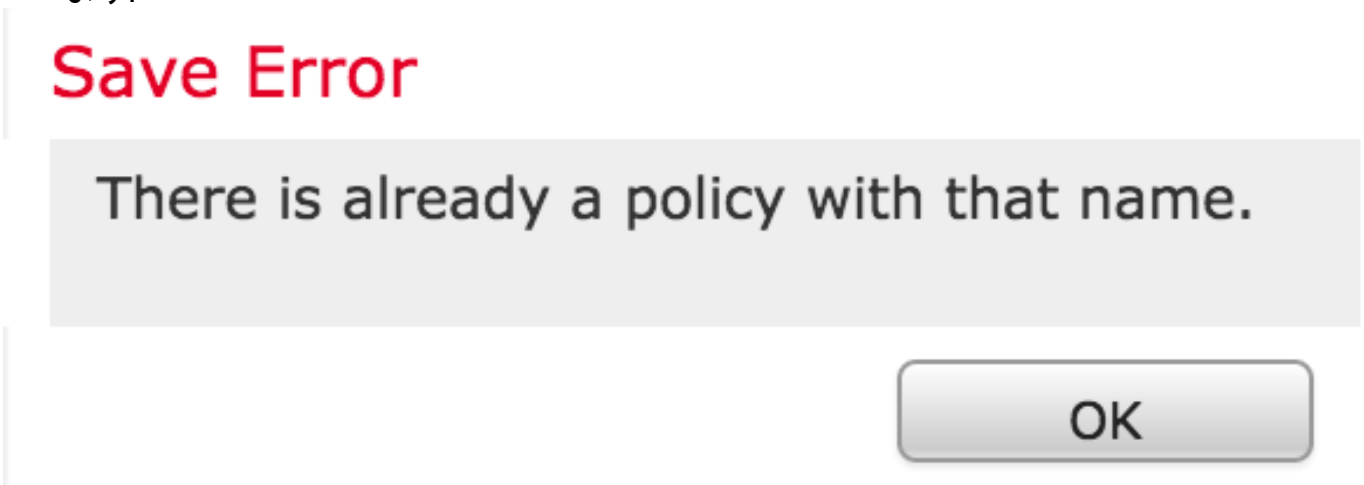
- ユーザポリシーのユーザ エージェント 情報
- NMAP スキャン
- 応答グループ
- 治療モジュール
- 治療例
- Estreamer およびホスト 入力 クライアント
- バックアップ プロファイル
- スケジュール
- ライセンス

- アップデート
- 健全性アラート

設定

高可用性を設定する前提条件

- デバイスは同じソフトウェア および ハードウェア バージョンである必要があります。
- インストールされるデバイスは同じ VDB がなければなりません。
- デバイスは同じ SRU がなければなりません。
- 両方の防御センターを持っていますアドミニストレーター特権の admin と指名されるユーザアカウントを確認して下さい。 これらのアカウントは同じパスワードを使用する必要があります。
- 管理者アカウント以外、2 つの防御センターに同一のユーザ名のユーザアカウントがないことを確認して下さい。 ハイ アベイラビリティを確立する前に重複したユーザー アカウントの 1 つを取除くか、または名前を変更して下さい。
- 両方のデバイスを持っていません同じ名前のアクセスコントロール ポリシーを確認して下さい。 同じ名前の 2 つのアクセスコントロール ポリシーがあればそれら両方は DC で共存します。 ただし、それらはデバイスを対応づけられることができません。ターゲットデバイスを追加した後このポリシーを保存すれば、この設定はイメージに示すようにエラーと拒否されます:



- 防御センターは両方ともインターネットにアクセスできなければなりません。

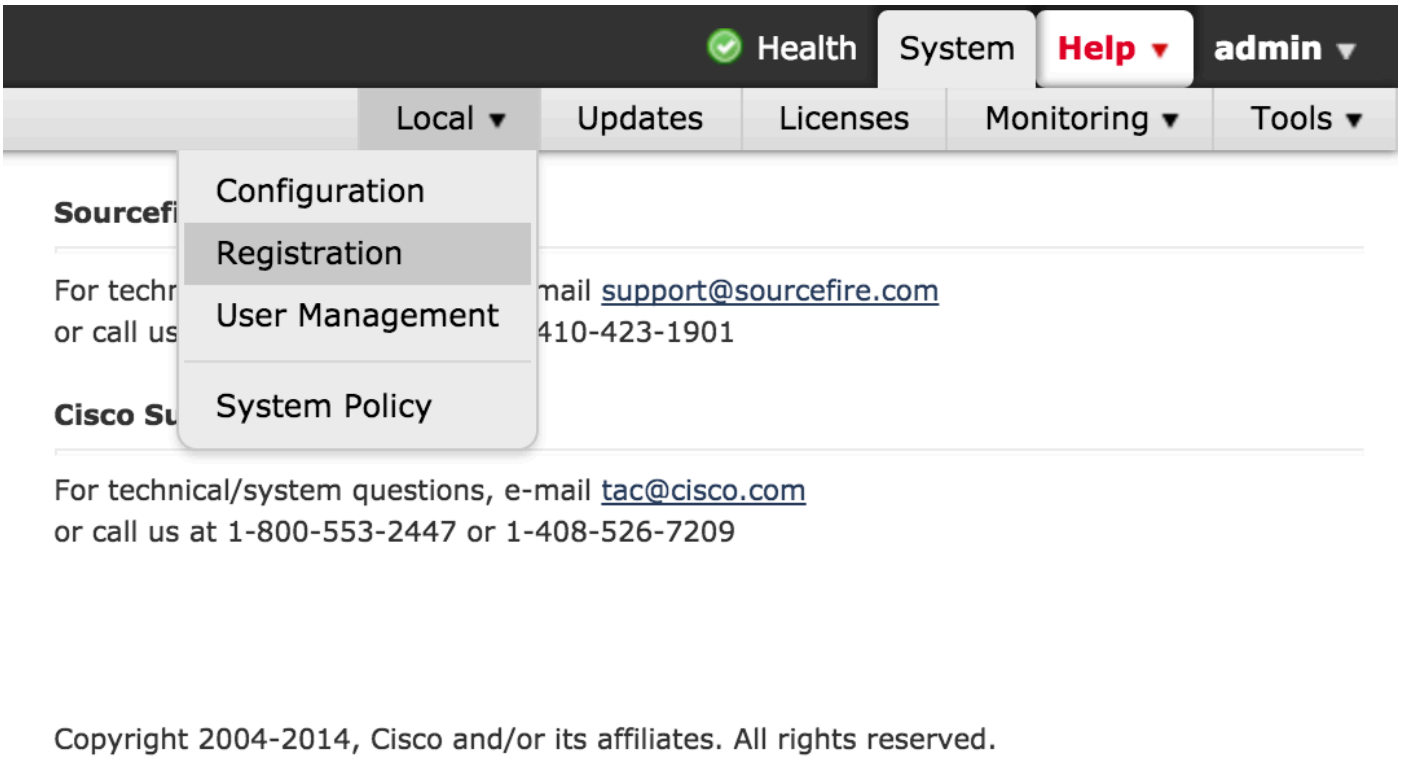
設定 高可用性

これらは高可用性を設定する 8 つのステップです。

ステップ 1. VDB バージョンと共にソフトウェア および ハードウェア バージョンおよびルール更新バージョンが同じであることを確認して下さい。

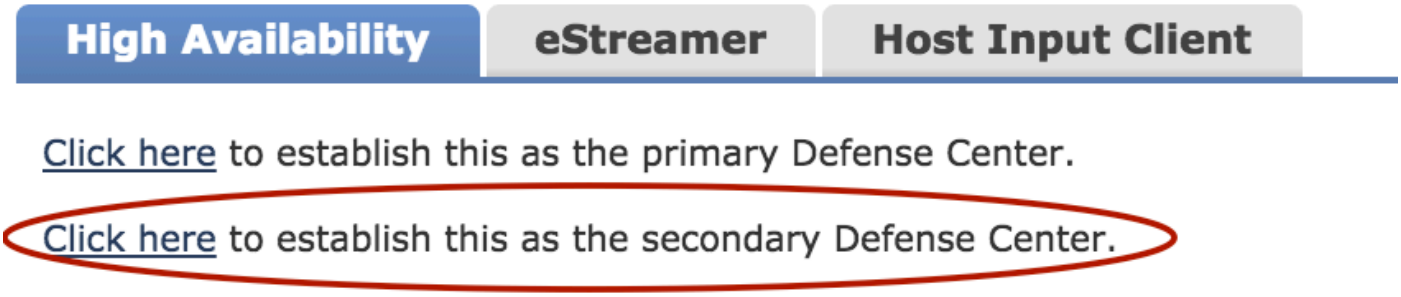
Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build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

ステップ 2.デバイス セカンダリを、ナビゲート、イメージに示すように**システム > ローカル > 登録**に作るため。 この DC の設定がないことを確認して下さい。

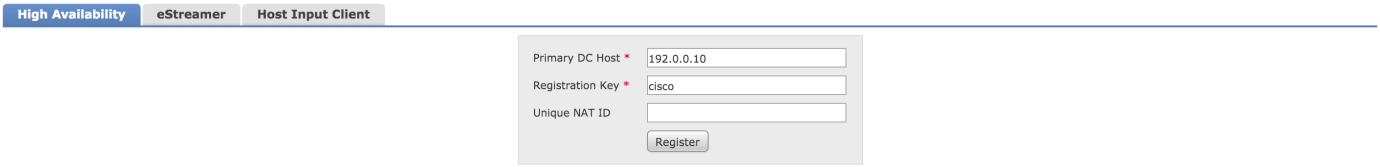


ステップ 3 **高可用性の**タブの下でイメージに示すように**セカンダリ防衛センターとしてこれを、**

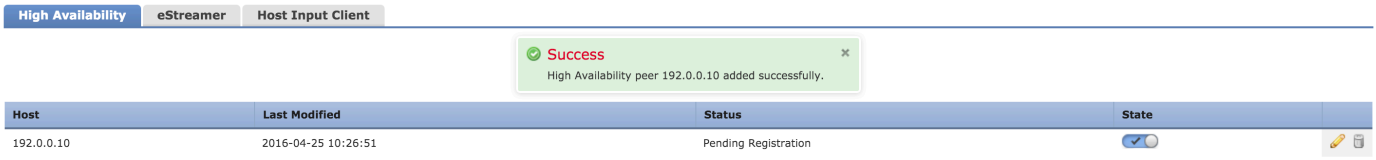
確立するために『Click Here』 をクリック して下さい:



ステップ 4 ステップ 3 を完了するので、ページはイメージに示すように表示する。 プライマリ DC およびパス キーの IP を追加して下さい。 a の後ろにネットワーク アドレス変換 (NAT) あるデバイスのためのユニークな NAT ID を追加するようにして下さい。



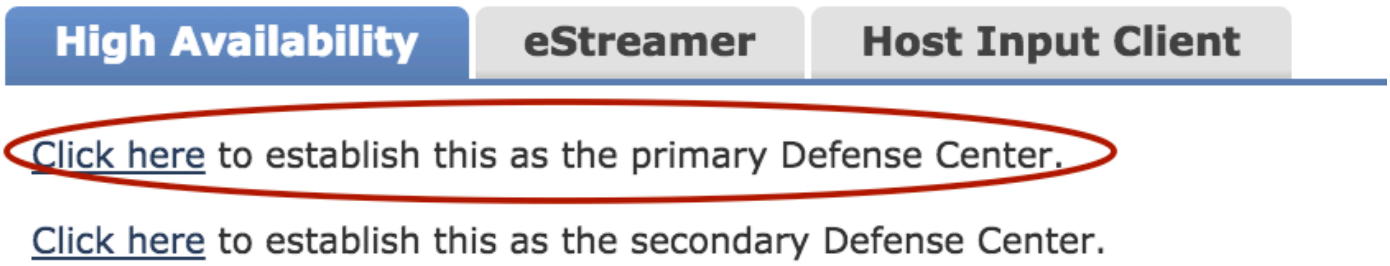
ステップ 5 IP アドレスが確認された後、正しかったら場合『register』 をクリック します。 イメージに示すようにページを見ます:



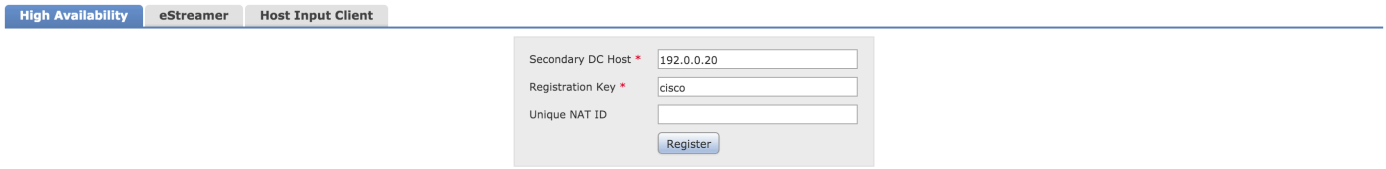
これは HA がセカンダリ DC で設定され、プライマリ DC でそれを設定する必要があることを意味します。

ステップ 6.プライマリ DC で設定したいデバイスへのログイン。 [System] > [Local] > [Registration] に移動します。

高可用性のタブの下でイメージに示すように**プライマリ防衛 センターとして、追加するために**『Click Here』 をクリック して下さい:

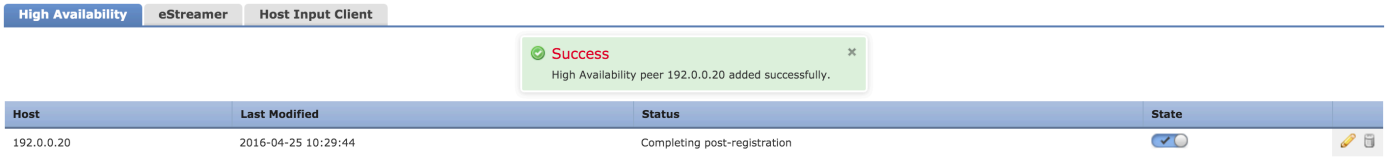


ステップ 7 ステップ 6 を完了した後、ページはイメージに示すように表示する:



セカンダリ DC IP を追加して下さい。 同じ登録 キーをおよびセカンダリ DC を設定する間、提供された NAT ID を提供します。

ステップ 8 IP の詳細の後で『register』 をクリック します確認されます。 登録が完了した、成功ページはイメージに示すように見られます:



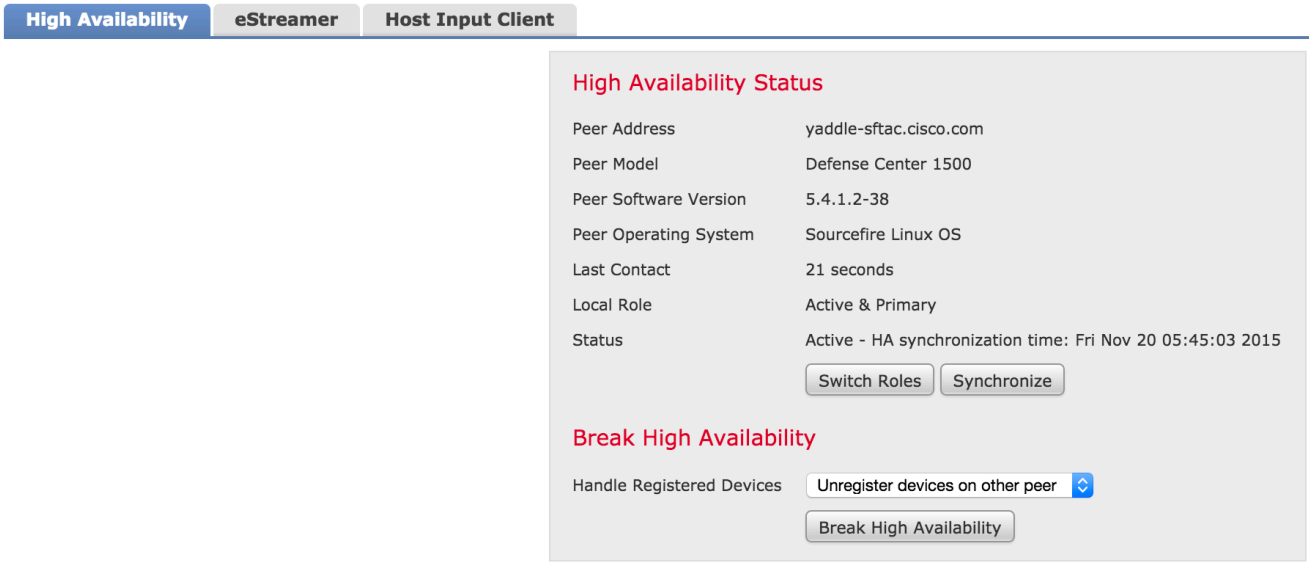
5-10 分後に HA 設定および同期は完了します。

ほぼ HA の設定および同期を完了するために 5-10 分かかります

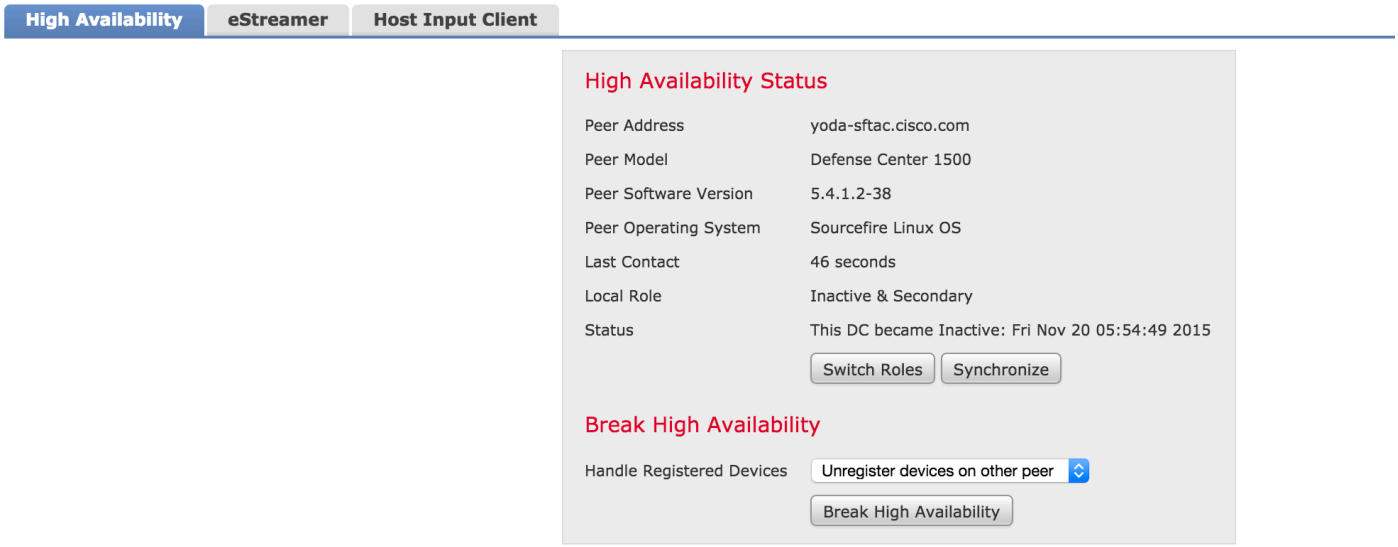
確認

DC がハイ アベイラビリティのために正しく設定されることを確認するステップバイステップ設定。

ステップ 1.イメージに示すようにプライマリデバイスの**システム >Local >Registration** にナビゲート して下さい:



ステップ 2.イメージに示すようにセカンダリデバイスの**システム >Local >Registration** へのナビゲート:



トラブルシューティング

このセクションはハイ アベイラビリティに基本的な トラブルシューティング の 手順を提供します。

- 情報およびハートビートを同期するのに HA がこのポートを使用するので、DC が TCPポート 8305 で受信している両方とも確認して下さい。
- TCPポート 8305 をブロックされませんネットワークでまたはあらゆる中間デバイスによって確認して下さい。
- HA 作成は削除されるか、または取り替えられる前のピアデバイスの古いエントリがある場合失敗します。 EM_Peers 表はそのようなピアデバイスで詳細を提供したものです。

関連情報

- Cisco Firepower 8000 シリーズ デバイスでのスタック設定
- Firesight システムユーザ ユーザーズ ガイド 5.4.1
- テクニカルサポートとドキュメント - Cisco Systems