Configuração da Alta disponibilidade na série 3 centros da defesa

Índice

Introdução

Este documento descreve a configuração de Availability(HA) alto para a defesa Centers(DC) da série 3.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia da potência de fogo
- Alta disponibilidade básica dos conceitos

Componentes Utilizados

A informação neste documento é baseada na versão de software sendo executado 5.3 dos dispositivos da série 3 do centro da defesa da potência de fogo (DC1500,DC2000,DC3500,DC4000) à versão de software 5.4.1.6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Para assegurar a continuidade das operações, a Alta disponibilidade da característica permite que você designe centros redundantes da defesa para controlar dispositivos. O centro da defesa mantém córregos de dados de evento dos dispositivos gerenciado e de determinados elementos de configuração destes dispositivos. Se uma defesa Center falha, você pode monitorar sua rede sem interrupção através do outro centro da defesa.

Alta disponibilidade das características

- A sincronização HA é bidirecional que significa mesmo que haja um preliminar e um dispositivo secundário designados, as mudanças adicionadas em qualquer dos dispositivos replicated ao outro.
- O HA não exige os dispositivos ser conectado diretamente. A conexão HA pode ser feita sobre um interruptor mas esta conexão precisa de estar no mesmo domínio de transmissão.
- Os dispositivos HA comunicam-se sobre seu IP de gerenciamento na porta 8305.
- O tempo de sincronização HA para um dispositivo é cinco minutos, assim que significa que depois que cada cinco minuto tentativas de um dispositivo de sincronizar sua configuração com seu par. Desde o tempo exigido para a sincronização é específico aos dispositivos, cumulativamente, o tempo de sincronização pode ser maximizado a dez minutos.
- Se uma nova imagem é exigida para um par específico HA recomenda-se quebrar o HA e então a nova imagem.
- Se você planeia promover o conjunto HA não é necessário quebrar o HA. Quando você promove da versão 5.3.0 à 5.4.0, promova os dispositivos um por um e uma vez que são promovidos execute uma tarefa da sincronização no centro da defesa principal.
- A presença de uma política de acesso com o mesmo nome em ambos os DC cria duas políticas do controle de acesso do mesmo nome. Uma política é configurada localmente e a outro é sincronizada do par DC.

  Nota: Você não pode adicionar um alvo ou aplicar esta política porque joga acima um erro, que indique que há já uma política com o mesmo nome.
- As licenças não são sincronizadas entre pares DC, consequentemente, são exigidas ser adicionadas separadamente aos DC.
- Todos os dispositivos gerenciado são adicionados somente a um DC. A configuração é sincronizada entre o par DC.
- Os dispositivos gerenciado enviam logs a ambos os DC.
- Os DC sincronizam as ações as mais atrasadas. Por exemplo, se você suprime de um usuário de DC-1, o outro par DC-2 não sincroniza a configuração do usuário a DC-1.

Sincroniza a **ação da supressão** e o usuário é perdido de DC-1 & de DC-2.

Configuração compartilhada bidirecional entre pares

Políticas dos sincronizars HA DC bidirecional. Estas configurações são sincronizados bidirecional entre pares. Você pode igualmente ver a maioria destas configurações com o trajeto definidas certo ao lado dele:

Identidades e autenticação

- A configuração externo LDAP navega ao **sistema > ao Local > ao gerenciamento de usuário > à autenticação externa**
- Usuários (interno e externo) - Navegue o toSystem **> os usuários de Management> do usuário de Local>**
- Os papéis de usuário feitos sob encomenda navegam o toSystem **> o Local > o gerenciamento de usuário > os papéis de usuário**

Relatórios

- Os moldes do relatório navegam à **vista geral > ao relatório > aos templates de relatório**

Políticas configuráveis (sob a seção das políticas)

- Políticas do controle de acesso, políticas da intrusão, políticas do arquivo, de políticas SSL políticas, de acesso de rede, políticas e regras da correlação, whitelist da conformidade e perfis de tráfego.
- Regras da intrusão (Local e SRU) - navegue toPolicies **> editor da regra de Intrusion> > regras locais.**
- Descoberta da rede, atributos do host, feedback de usuário da descoberta da rede, incluindo notas e criticidade do host, o supressão dos anfitriões, aplicativos, e redes do mapa de rede e a desativação ou a alteração das vulnerabilidades.
- Detectores feitos sob encomenda do aplicativo
- As conexões ldap em políticas do usuário navegam toPolicies **> usuários**
- Os alertas navegam às **ações > aos alertas de Policies>** (sob respostas)

Informação do dispositivo

- As regras NAT navegam toDevices **> NAT**
- As regras VPN navegam toDevices **> VPN**
- Toda a informação do dispositivo que inclui o nome e seu grupo é sincronizado bidirecional. O lugar para o armazenamento do log para cada dispositivo é igualmente sincronizado entre pares - navegue toDevices **> Gerenciamento de dispositivos**
- Classificações feitas sob encomenda da regra da intrusão
- Impressões digitais feitas sob encomenda ativadas
- Política de sistema e política sanitária
- Painéis feitos sob encomenda, trabalhos feitos sob encomenda e tabelas feitas sob encomenda
- Mude a reconciliação, os instantâneos e os ajustes do relatório
- Base de dados das atualizações (SRU), do Geolocation da regra de Sourcefire (GeoDB), e atualizações do base de dados da vulnerabilidade (VDB)

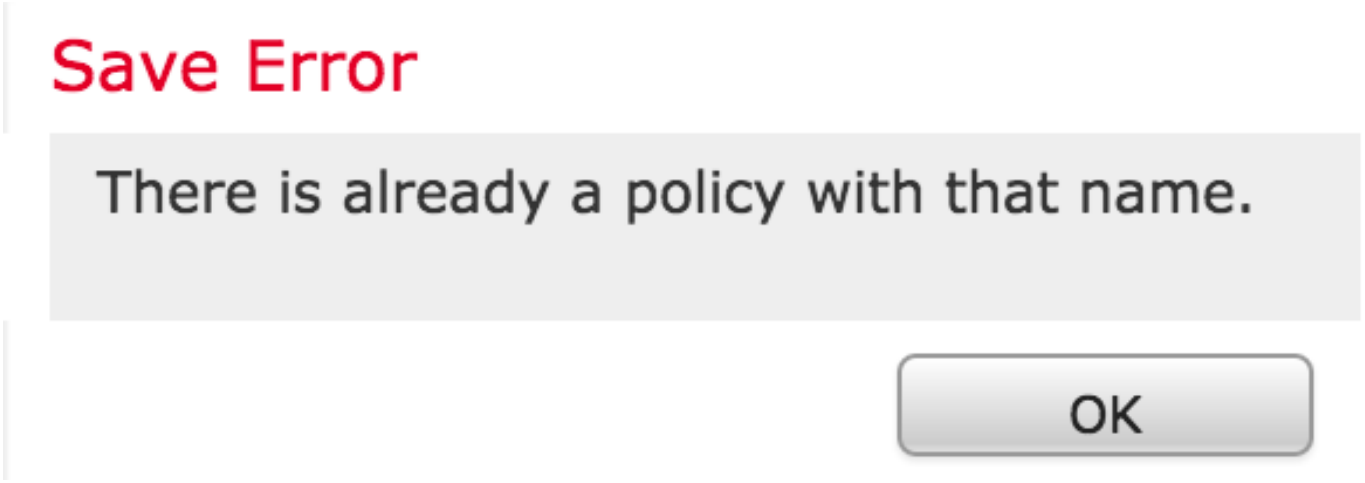
Configuração não sincronizado entre DC

- Informação do agente de usuário na política de usuário
- Varreduras NMAP
- Grupos da resposta
- Módulos da remediação
- Exemplos da remediação
- Estreamer e cliente da entrada do host
- Perfis alternativos
- Programações
- Licenças
- Atualizações
- Alertas da saúde

Configurar

Condições prévias para configurar a Alta disponibilidade

- Os dispositivos devem ser da mesma versão de software e hardware.
- Os dispositivos devem ter o mesmo VDB instalados.
- Os dispositivos devem ter o mesmo SRU.
- Assegure-se de que ambos os centros da defesa tenham uma conta de usuário nomeada admin com privilégios do administrado. Estas contas devem usar a mesma senha.
- Assegure-se de que a não ser a conta admin, os dois centros da defesa não tenham contas de usuário com nomes de usuário idênticos. Remova ou rebatize uma da conta de usuários duplicada antes que você estabeleça a Alta disponibilidade.
- Assegure-se de que ambos os dispositivos não tenham nenhuma políticas do controle de acesso com o mesmo nome. Se há duas políticas do controle de acesso com o mesmo nome eles ambos coexistem nos DC. Contudo, não podem obter associados com nenhum dispositivo. Uma vez que você salvar esta política após ter adicionado um dispositivo de destino, esta configuração está rejeitada com um erro segundo as indicações da imagem:



- Ambos os centros da defesa devem ter o acesso ao Internet.

Configurar a Alta disponibilidade

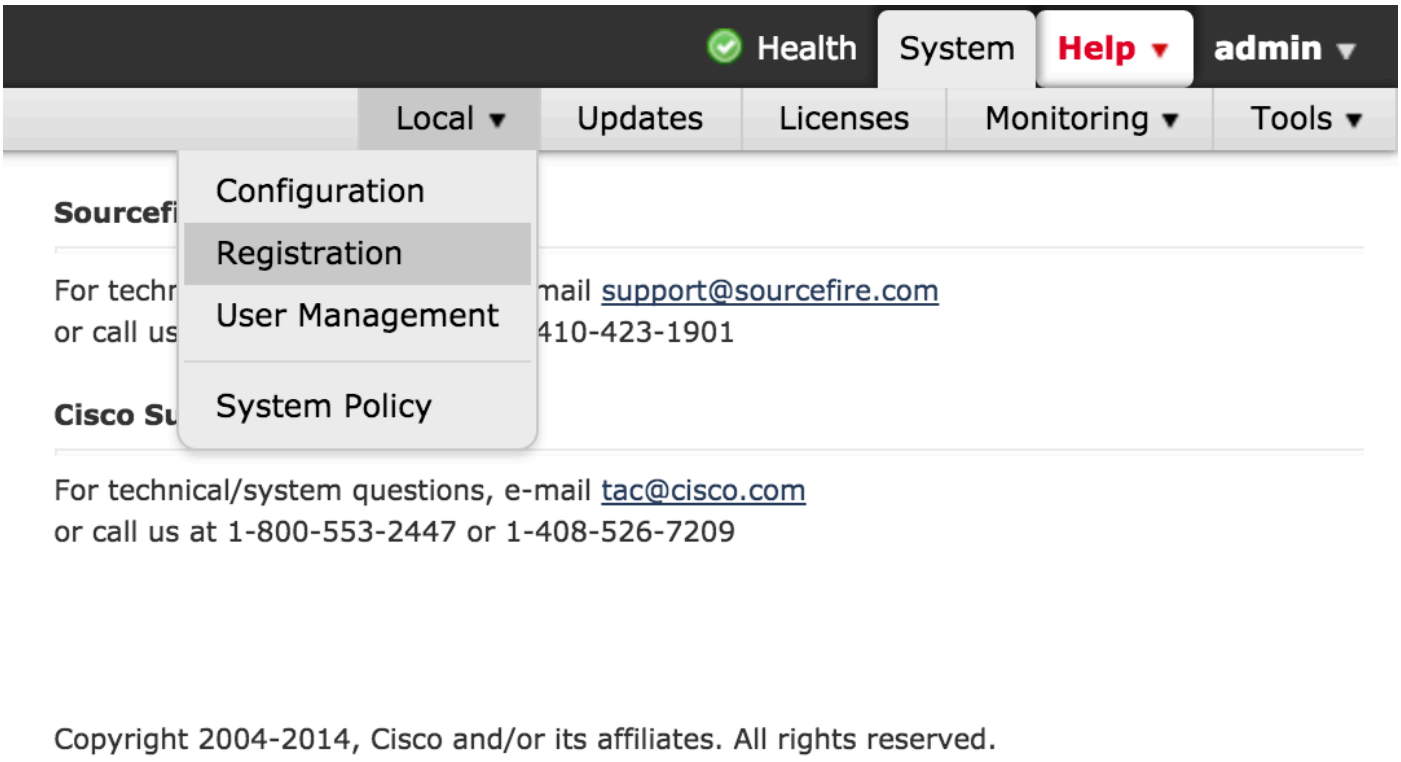
Estas são as 8 etapas para configurar a Alta disponibilidade.

Etapa 1. Confirme que a versão de software e hardware junto com a versão VDB e a versão da atualização da regra são a mesma.

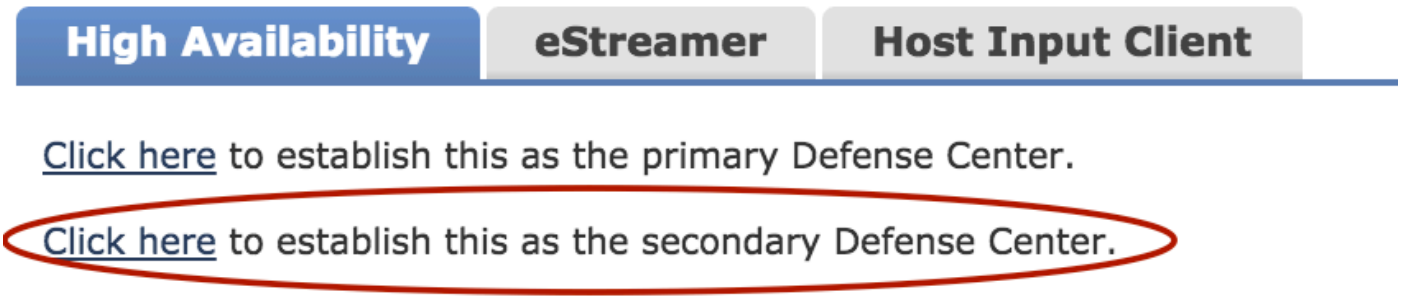
Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build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

Etapa 2. A fim fazer seu dispositivo secundário, navegue ao **sistema > ao Local > ao registro**, segundo as indicações da imagem. Assegure-se de que você não tenha nenhuma configuração

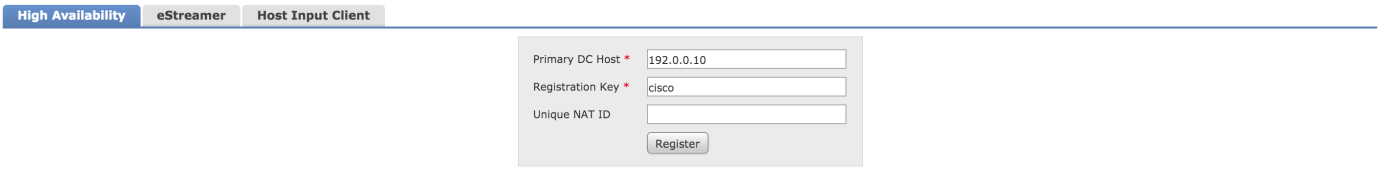
neste DC.



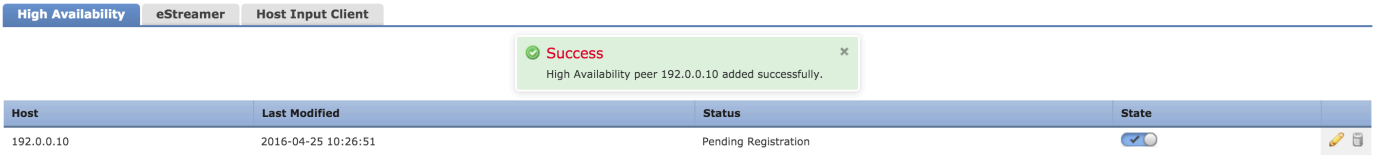
Etapa 3. Sob a **Alta disponibilidade da** aba clique **clicam** sobre **aqui para estabelecer isto como um centro secundário da defesa**, segundo as indicações da imagem:



Etapa 4. Porque você termina etapa 3, uma página é indicada segundo as indicações da imagem. Adicionar o IP do DC preliminar e da chave da passagem. Assegure-se de que você adicione um ID do NAT original para os dispositivos, que são atrás de uma tradução de endereço de rede.



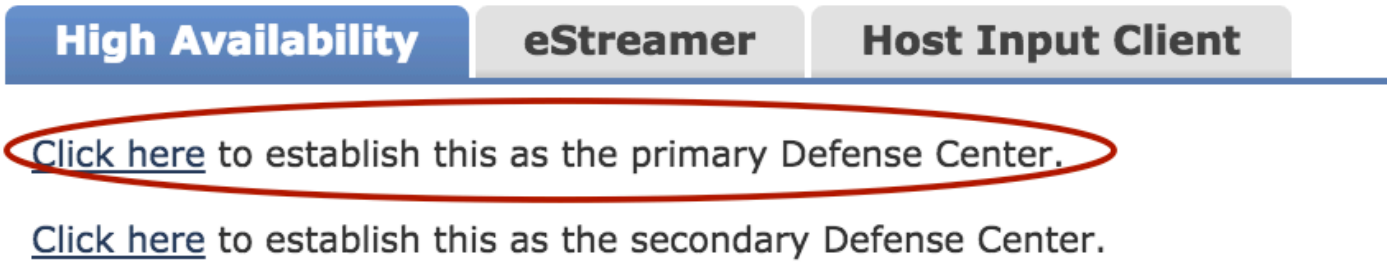
Etapa 5. Depois que o endereço IP de Um ou Mais Servidores Cisco ICM NT é verificado, se correto clique sobre o **registro**. Você vê uma página segundo as indicações da imagem:



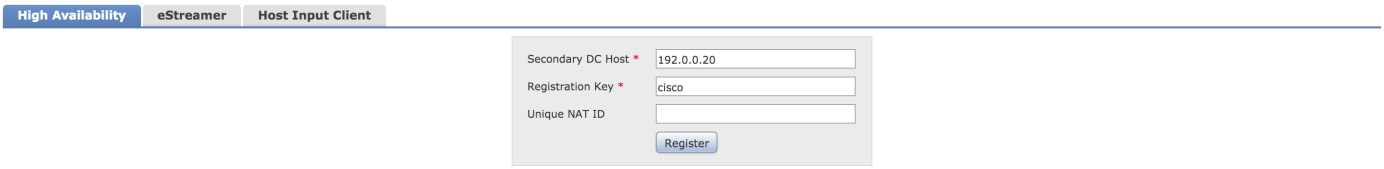
Isto significa que o HA está configurado no DC secundário e você precisa do configurar no DC preliminar.

Etapa 6. Início de uma sessão ao dispositivo que você deseja configurar como o DC preliminar. Navegue ao **sistema > ao Local > ao registro.**

Sob a **Alta disponibilidade da** aba clique **clicam** sobre **aqui para adicionar como o centro da defesa principal**, segundo as indicações da imagem:

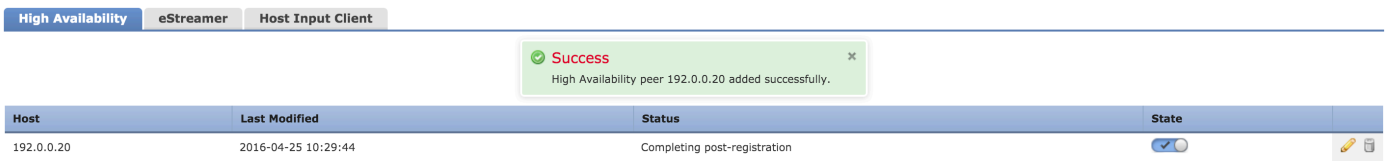


Etapa 7. Depois que você termina a etapa 6, uma página está indicada segundo as indicações da imagem:



Adicionar o IP secundário DC. Forneça a mesma chave do registro e a identificação NAT que foi fornecida quando você configurou o DC secundário.

Etapa 8. Depois que os detalhes do IP são verificados clique sobre o **registro.** Uma vez que o registro está completo, a página do sucesso está vista segundo as indicações da imagem:



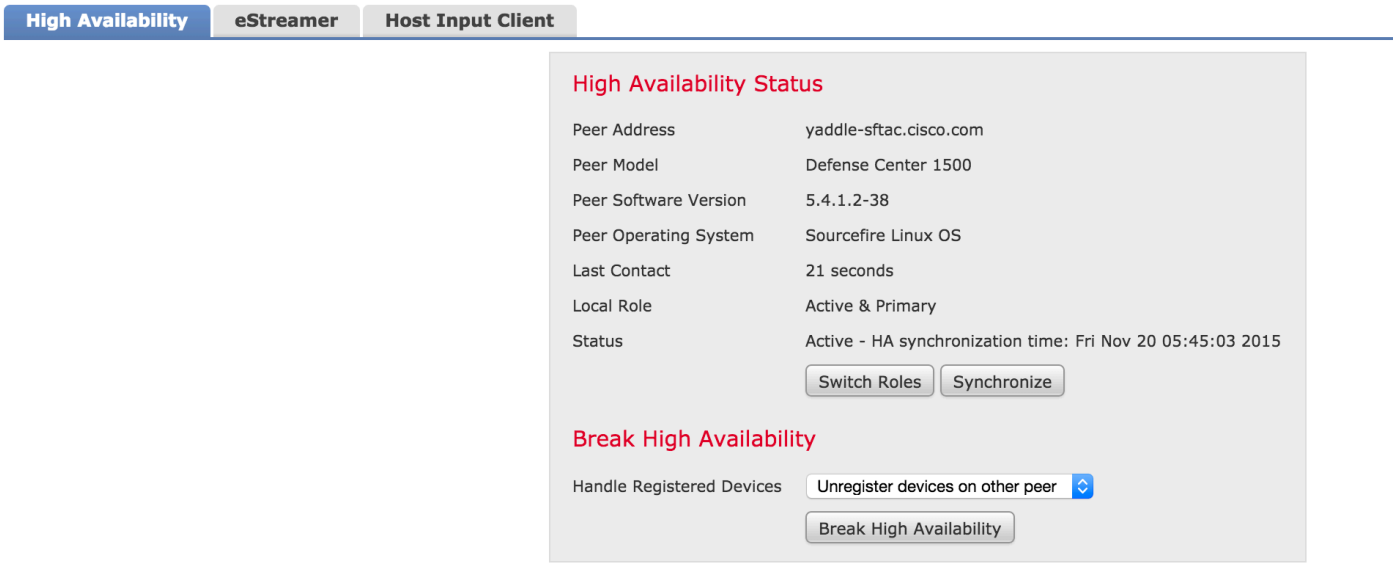
Após 5-10 os minutos HA a configuração e a sincronização são terminadas.

Toma quase 5-10 minuto a fim terminar a configuração e a sincronização do HA

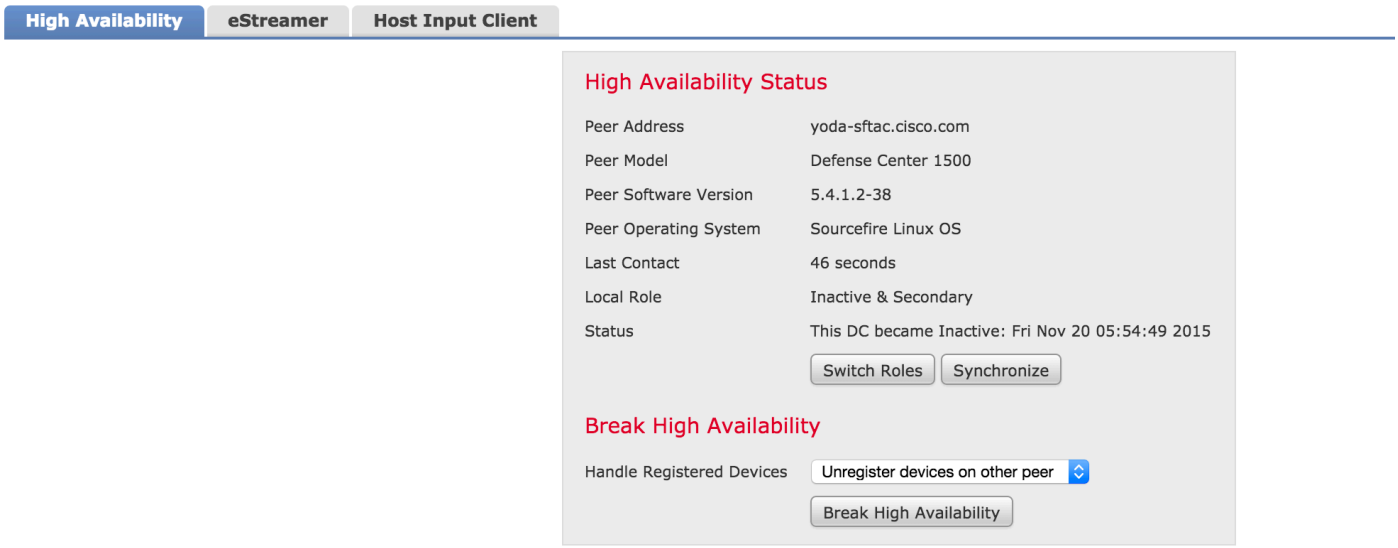
Verificar

Configuração passo a passo para verificar que seus DC estão configurados corretamente para a Alta disponibilidade.

Etapa 1. Navegue ao **>Registration >Local do sistema no** dispositivo principal segundo as indicações da imagem:



Etapa 2. Navegue ao **>Registration >Local do sistema no** dispositivo secundário segundo as indicações da imagem:



Troubleshooting

Esta seção fornece etapas de Troubleshooting básicas para a Alta disponibilidade.

- Assegure-se de que ambos os DC estejam escutando na porta TCP 8305, desde que o HA usa esta porta para sincronizar a informação e as pulsação do coração.
- Assegure-se de que a porta TCP 8305 não esteja obstruída na rede ou por nenhuns dispositivos intermediários.
- A criação HA falha se há uma entrada velha de um dispositivo de peer precedente que esteja removido ou substituído. A tabela de EM_Peers fornece mais informação em tais dispositivos de peer.

Informações Relacionadas

- Configuração da pilha nos dispositivos do 8000 Series da potência de fogo de Cisco
- Guia de usuário de sistema 5.4.1 de Firesight
- Suporte Técnico e Documentação - Cisco Systems