Конфигурация высокой доступности на серии 3 центра защиты

Содержание

Введение

Этот документ описывает конфигурацию Высокой доступности (HA) для Серии 3 Центра защиты (DC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Технология огневой мощи
- Основные понятия высокой доступности

Используемые компоненты

Сведения в этом документе основываются на Серии Центра Защиты Огневой мощи 3 устройства (DC1500, DC2000, DC3500, DC4000) работающий от версии программного обеспечения 5.3 до версии программного обеспечения 5.4.1.6

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Для обеспечения непрерывности операций функция обеспечения высокой доступности позволяет вам определять избыточные Центры Защиты управлять устройствами. Центр Защиты поддерживает потоки данных события от управляемых устройств и определенных элементов конфигурации этих устройств. Если один Центр Защиты отказывает, можно контролировать сеть без прерывания через другой Центр Защиты.

Функции обеспечения высокой доступности

- HA синхронизация является двунаправленной, что означает даже при том, что существует определяемый основной и дополнительное устройство, изменения прибавили любое из устройств, реплицированы в другой.

- HA не требует, чтобы напрямую подключились устройства. Соединение HA может быть сделано по коммутатору, но это соединение должно быть в том же широковещательном домене.

- HA устройства связываются по их IP - управлению в порту 8305.

- HA время синхронизации для устройства составляет пять минут, что означает, что после каждых пяти минут устройство пытается синхронизировать свою конфигурацию с его узлом. Так как время, требуемое для синхронизации, является определенным для устройств, кумулятивно, время синхронизации может быть увеличено к десяти минутам.

- Если повторно захватывание образ требуется для определенного узла HA, рекомендуется сломать HA и затем повторно захватить образ.

- Если вы планируете обновить кластер HA необязательно для ломки HA.When, вы обновляете от версии 5.3.0 до 5.4.0, обновляете устройства один за другим и как только они обновлены, выполняют задачу синхронизации на Центре основного метода защиты.

- Присутствие политики доступа с тем же названием на обоих DC создает две Политики контроля доступа того же названия. Одна политика настроена локально, и другой синхронизируется от однорангового DC.

  Примечание: Вы не можете добавить цель или применить эту политику , потому что она подбрасывает ошибку, которая сообщает, что уже существует политика с тем же названием.

- Лицензии "not synchronized" между узлами DC, поэтому, они обязаны быть добавленными отдельно к DC.

- Все управляемые устройства добавлены только к одному DC. Конфигурация синхронизируется между одноранговыми DC.

- Управляемые устройства передают журналы обоим DC.

- DC синхронизируют последние действия. Например, при удалении пользователя из DC1 другой одноранговый DC 2 не синхронизирует пользовательскую конфигурацию с DC1. Это синхронизирует **удалить действие**, и пользователь потерян от обоих DC1 и DC 2.

Конфигурация, разделенная двунаправленным образом между узлами

HA DC синхронизируют политику двунаправленным образом. Эти конфигурации синхронизируются двунаправленным образом между узлами. Можно также просмотреть большинство этих конфигураций с путем, определенным прямо рядом с ним:

Личности и аутентификация

- Внешняя Конфигурация LDAP - Перешла к **Системе> Локальный> Управление пользователями> Внешняя проверка подлинности**
- Пользователи (Внутренний и Внешний) - Перемещаются по toSystem**> Локальный>> Users Управления пользователями**
- Пользовательские Роли пользователя - Перемещаются по toSystem**> Локальный> Управление пользователями> Роли пользователя**

Отчёты

- Шаблоны отчета - Перешли к **Обзору> Сообщающий> Шаблоны отчета**

Конфигурируемая политика (под разделом политики)

- Политика контроля доступа, Политика Проникновения, Политика Файла, Политика SSL, политика Доступа к сети, Политика Корреляции и правила, белый список Соответствия и профили трафика.
- Правила проникновения (Локальный и SRU) - Перемещаются по toPolicies**> Проникновение> Редактор Правила> Локальные Правила.**
- Обнаружение сети, атрибуты Хоста, обратная связь с пользователями Обнаружения сети, включая примечания и критичность хоста, удаление хостов, приложений и сетей от карты сети и деактивации или модификации уязвимостей.
- Детекторы пользовательского приложения
- Соединения LDAP в Пользовательской политике - Перемещаются **по toPolicies> Users**
- Предупреждения - Перешли к **Политике> Действия> Предупреждения** (При Ответах)

Сведения об устройстве

- Правила NAT - Перемещаются **по toDevices> NAT**
- Правила VPN - Перемещаются по toDevices**> VPN**
- Все сведения об устройстве включая название и его группу синхронизируются двунаправленным образом. Местоположение для хранения журналов для каждого устройства также синхронизируется между узлами - Перемещаются по toDevices**> Управление устройствами**
- Пользовательские классификации Правил Проникновения
- Активированные пользовательские отпечатки пальца
- Системная политика и Политика в области охраны здоровья
- Пользовательские информационные панели, Пользовательские потоки операций и пользовательские таблицы
- Согласование изменения, снимки и параметры настройки отчёта

- Обновления правила Sourcefire (SRU), база данных Геолокации (GeoDB) и база данных уязвимости (VDB) обновления

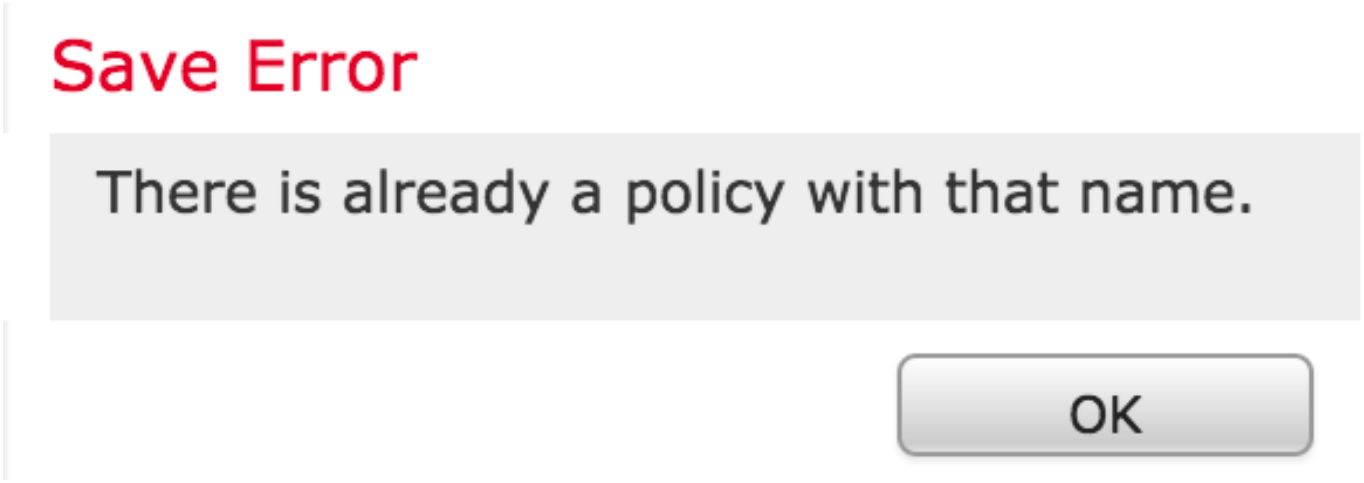
Конфигурация, не синхронизировавшая между DC

- Информация о Клиенте User Agent в Пользовательской политике
- Просмотры NMAP
- Response Groups
- Модули исправления
- Экземпляры исправления
- Estreamer и Host Input Client
- Резервные профили
- Списки
- Лицензии
- Обновления
- Предупреждения состояния

Настройка

Предварительные условия для настройки Высокой доступности

- Устройства должны иметь ту же версию программного и аппаратного обеспечения.
- Устройствам нужно было установить тот же VDB.
- Устройства должны иметь тот же SRU.
- Гарантируйте, что оба Центра Защиты имеют учетную запись пользователя, названную admin с Администраторскими привилегиями. Эти учетные записи должны использовать тот же пароль.
- Гарантируйте, что кроме учетной записи администратора, два Центра Защиты не имеют учетных записей пользователя с идентичными именами пользователей. Удалите или переименуйте одну из двойной пользовательской учетной записи перед установлением высокой доступности.
- Гарантируйте обоим, которых устройства не имеют никакой Политикой контроля доступа с тем же названием. Если существует две Политики контроля доступа с тем же названием, они оба сосуществуют на DC. Однако они не могут быть привязаны ни к какому устройству. Как только вы сохраняете эту политику после добавления устройства назначения, эта конфигурация отклонена с ошибкой как показано в образе:



- У обоих Центры Защиты должен быть доступ к Интернету.

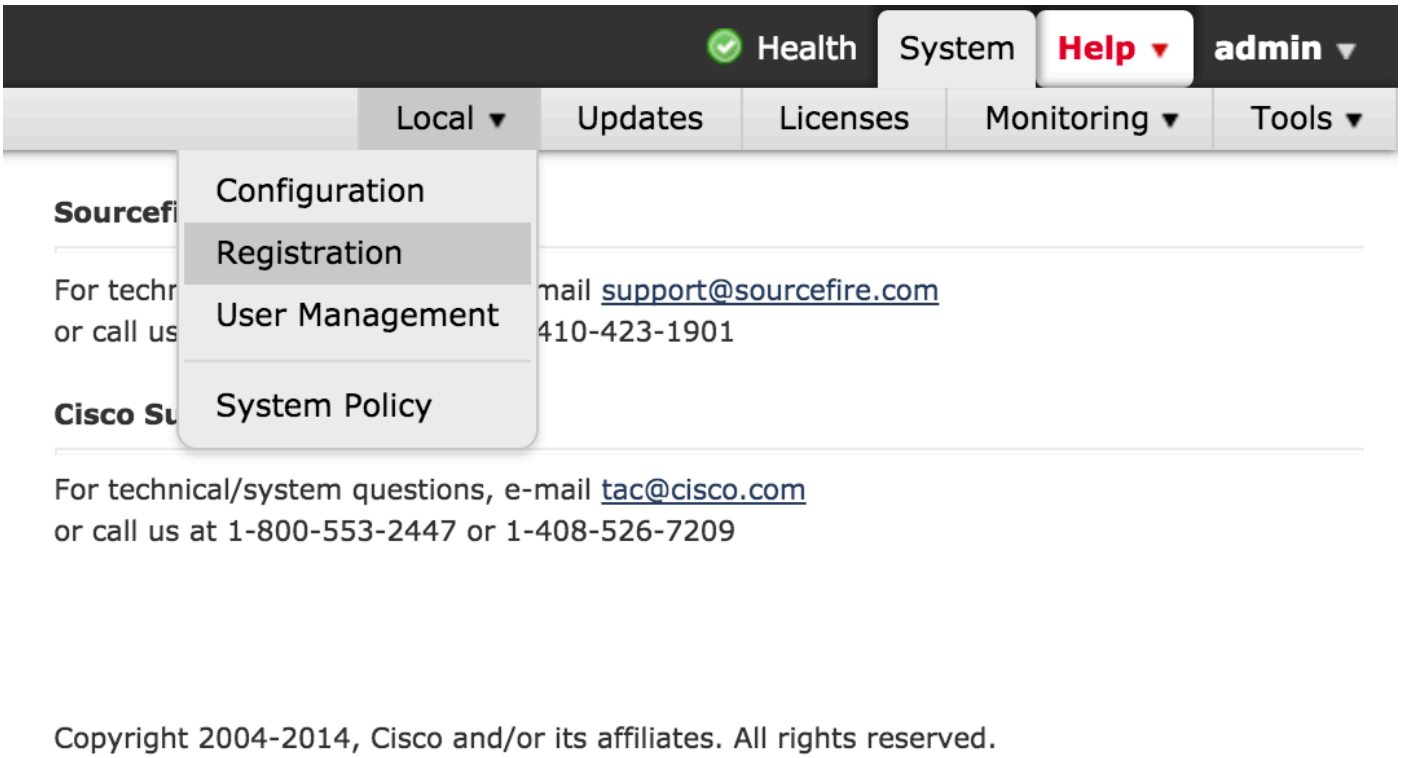
Настройте высокую доступность

Это 8 шагов для настройки Высокой доступности.

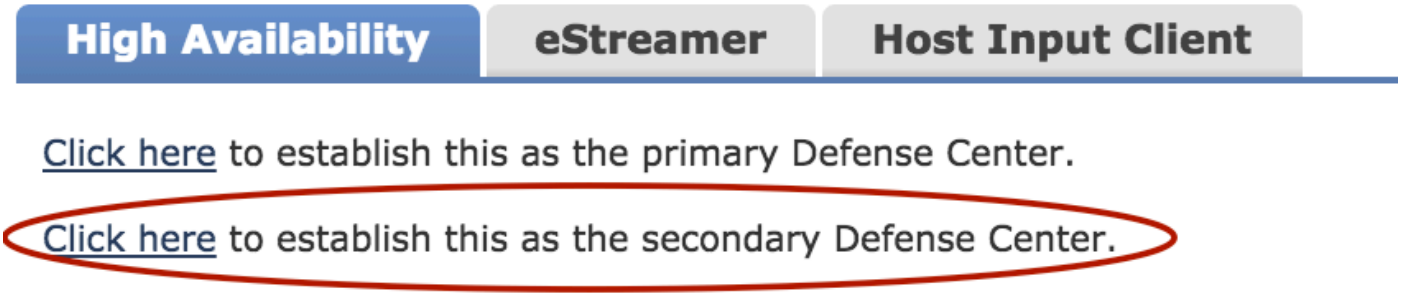
Шаг 1. Подтвердите, что версия программного и аппаратного обеспечения наряду с версией VDB и версией обновления правила является тем же.

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)

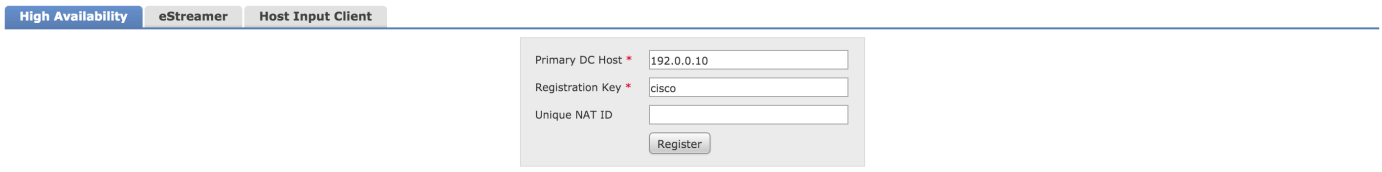
Шаг 2. Для создания устройства вторичным, перейдите к **Системе> Локальный> Регистрация**, как показано в образе. Гарантируйте, что у вас нет конфигурации на этом DC.



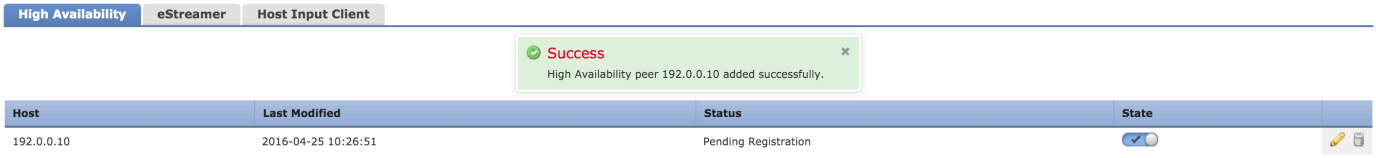
Шаг 3. Под Щелчком вкладки **High Availability по щелчку здесь для установления этого как вторичного Центра защиты**, как показано в образе:



Шаг 4. . Поскольку вы завершаете Шаг 3, страница отображена как показано в образе. Добавьте IP основного DC и ключа прохода. Гарантируйте добавление уникального КОДА NAT для устройств которые находятся позади Трансляции сетевых адресов.



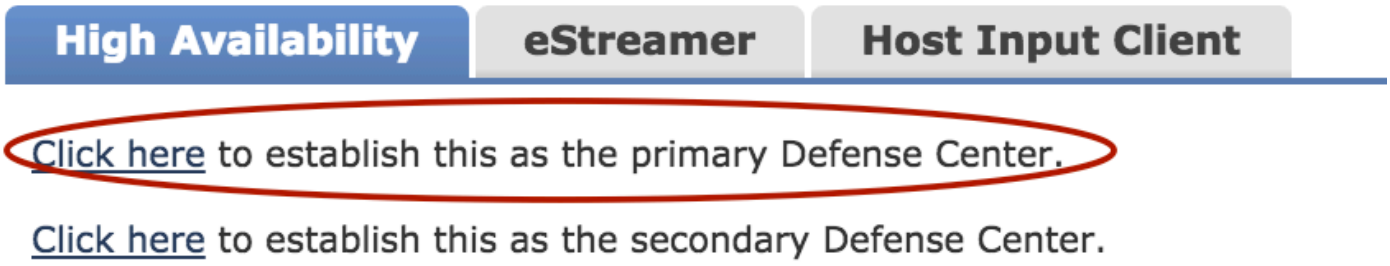
Шаг 5. . После того, как IP-адрес проверен, если корректный щелкните **по Register**. Вы видите страницу как показано в образе:



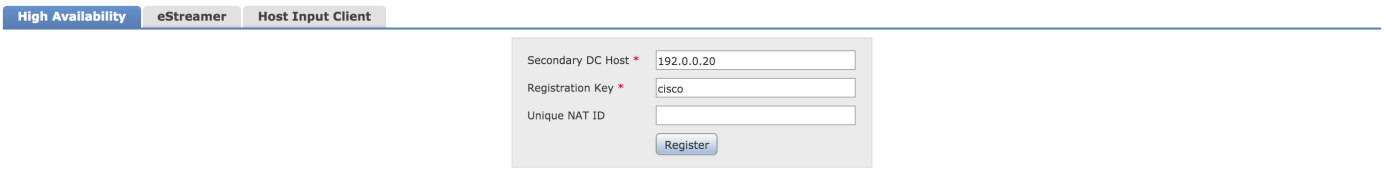
Это означает, что HA настроен на Вторичном DC, и необходимо настроить его на Основном DC.

Шаг 6. Войдите к устройству, которое вы хотите настроить как основной DC. Перейдите к **Системе> Локальный> Регистрация.**

Под Щелчком вкладки **High Availability по щелчку здесь для добавления как Центр основного метода защиты**, как показано в образе:

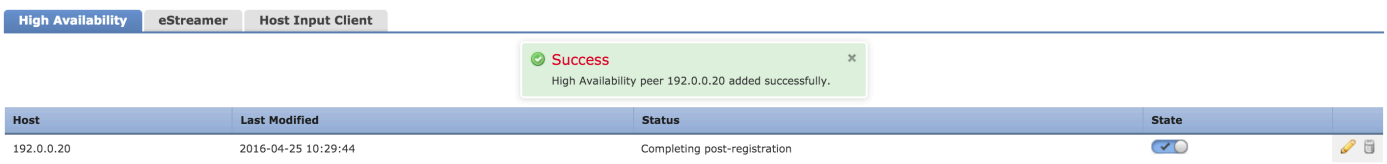


Шаг 7. После завершения Шага 6 страница отображена как показано в образе:



Добавьте Вторичного IP DC. Предоставьте тот же регистрационный ключ и код NAT, который был предоставлен, в то время как вы настроили вторичный DC.

Шаг 8. После того, как подробные данные IP проверены, щелкают **по Register.** Как только регистрация завершена, страница Sucess замечена как показано в образе:



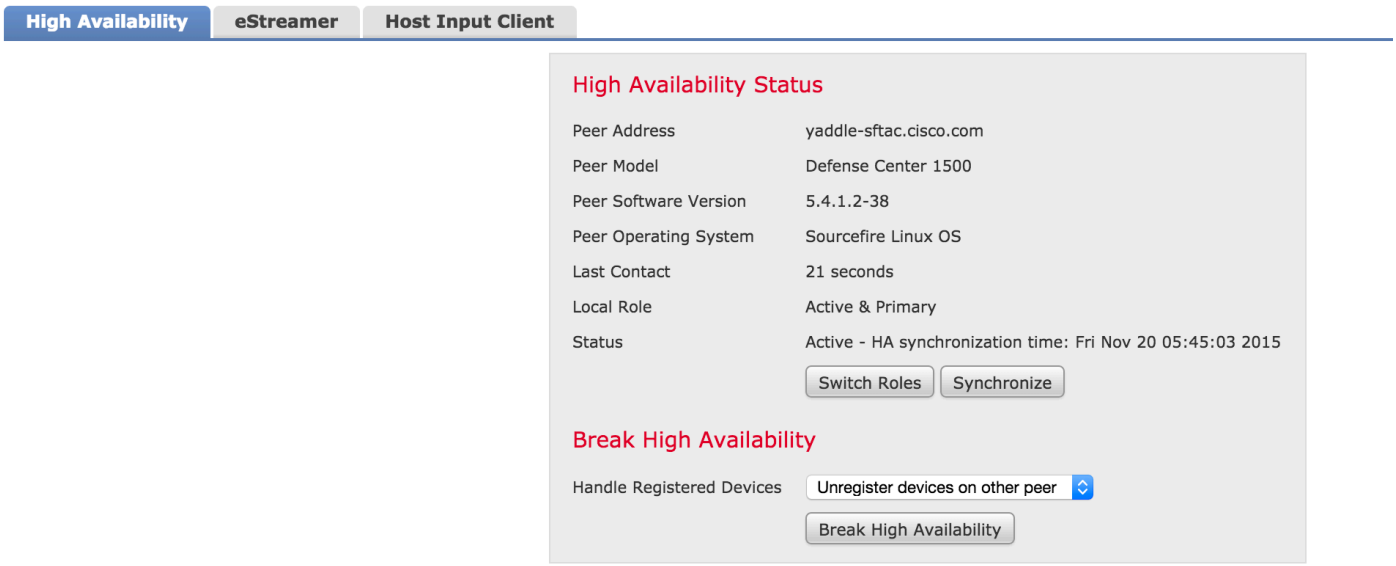
После 5-10 минут завершены конфигурация и синхронизация HA.

Требуется почти 5-10 минут для завершения конфигурации и синхронизации HA

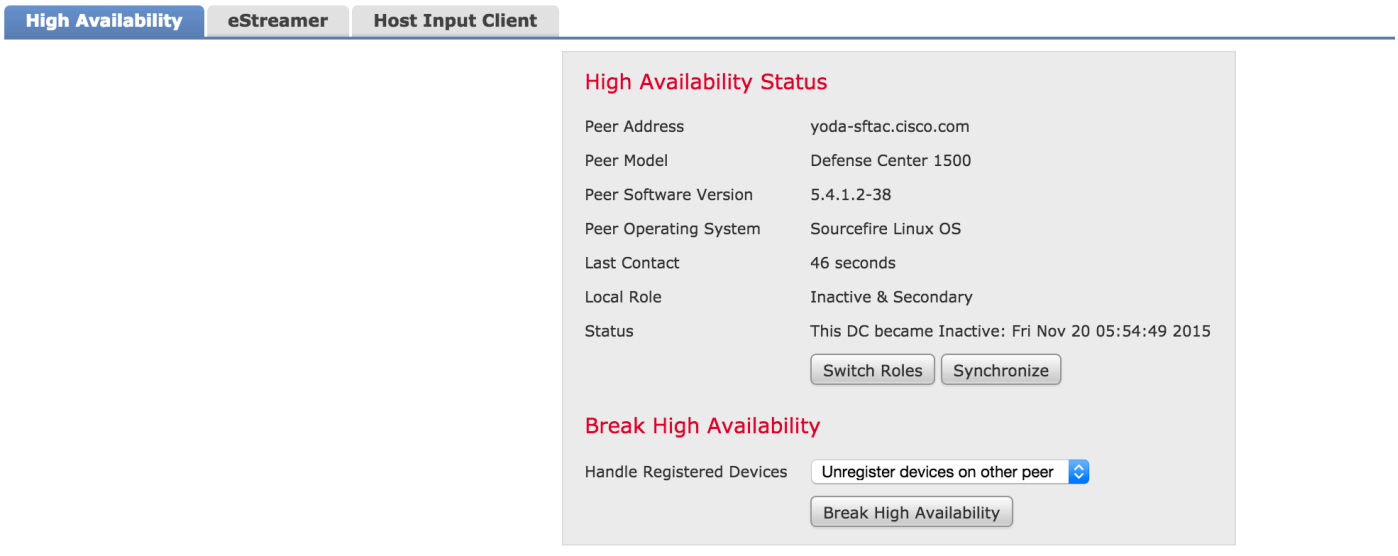
Проверка

Пошаговая конфигурация, чтобы проверить, что ваш DC настроен правильно для высокой доступности.

Шаг 1. Перейдите к **Системе> Локальный> Регистрация** на основном устройстве как показано в образе:



Шаг 2. Перейдите к **Системе> Локальный> Регистрация** на дополнительном устройстве как показано в образе:



Устранение неполадок

Этот раздел предоставляет основные действия по устранению проблем для высокой доступности.

- Гарантируйте обоим, которые DC слушает на порте TCP 8305, с тех пор HA использование этот порт для синхронизации информации и биений..
- Гарантируйте, что порт TCP 8305 не заблокирован в сети или никакими промежуточными устройствами.
- HA создание отказывает, если существует устаревшая запись предыдущего одноранговое устройства, которое демонтировано или заменено. Таблица EM_Peers предоставляет дополнительные сведения о таких одноранговых устройствах.

Дополнительные сведения

- Конфигурация стека на огневой мощи Cisco устройства серии 8000
- Руководство пользователя системы Firesight 5.4.1
- Cisco Systems – техническая поддержка и документация