تكوين التوافر العالي على سلسلة 3 لمراكز الدفاع

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
ميزات التوافر العالي
تمت مشاركة التكوين بشكل ثنائي الإتجاه بين النظراء
لم تتم مزامنة التكوين بين وحدات التحكم بالمجال DC
التكوين
المتطلبات الأساسية لتكوين التوافر العالي
تكوين التوافر العالي
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند تكوين التوفر العالي (HA) للسلسلة 3 من مراكز الدفاع (DC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تقنية Firepower
- المفاهيم الأساسية للتوفر العالي

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى أجهزة FirePOWER Defense Center Series 3 (DC1500،DC2000،DC3500،DC4000) التي تعمل من الإصدار 5.3 من البرنامج إلى الإصدار 5.4.1.6

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

ولضمان إستمرارية العمليات، تتيح لك ميزة "التوفر العالي" إمكانية تعيين مراكز الدفاع الاحتياطية لإدارة الأجهزة.يحتفظ "مركز الدفاع" بتدفقات بيانات الأحداث من الأجهزة المدارة وعناصر تكوين معينة من هذه الأجهزة. إذا فشل أحد مراكز الدفاع، يمكنك مراقبة شبكتك دون مقاطعة من خلال مركز الدفاع الآخر.

ميزات التوافر العالي

- إن مزامنة HA ثنائية الإتجاه وهذا يعني أنه على الرغم من وجود جهاز أساسي وثانوي محدد، فإنه يتم نسخ التغييرات التي تمت إضافتها على أي من الجهازين إلى الآخر.

- لا يتطلب HA توصيل الأجهزة مباشرة. يمكن إجراء اتصال HA عبر محول ولكن يلزم أن يكون هذا الاتصال في مجال البث نفسه.

- تتصل أجهزة HA عبر IP الخاص بإدارتها في المنفذ 8305.

- يبلغ وقت مزامنة HA للجهاز خمس دقائق، مما يعني أنه بعد كل خمس دقائق يحاول الجهاز مزامنة تكوينه مع نظيره. نظرا لأن الوقت المطلوب للمزامنة محدد للأجهزة، وبشكل تراكمي، يمكن زيادة وقت المزامنة إلى عشر دقائق.

- إذا كانت إعادة الصورة مطلوبة لنظير HA معين، فمن المستحسن كسر HA ثم إعادة تصويرها.

- إذا كنت تخطط لترقية مجموعة HA، فلن يكون من الضروري كسر HA .عند الترقية من الإصدار 5.3.0 إلى 5.4.0، قم بترقية الأجهزة واحدة تلو الأخرى وبمجرد ترقيتها، قم بتنفيذ مهمة مزامنة على مركز الدفاع الأساسي.
- يؤدي وجود نهج وصول بنفس الاسم على كلا وحدتي التحكم في الوصول إلى إنشاء نهج تحكم بنفس الاسم. يتم تكوين أحد النهج محليا ويتم مزامنة النهج الآخر من DC النظير.

ملاحظة: لا يمكنك إضافة هدف أو تطبيق هذا النهج لأنه يؤدي إلى حدوث خطأ، والذي يشير إلى وجود نهج بنفس الاسم بالفعل.

- لا تتم مزامنة التراخيص بين أقران DC، لذلك، يجب إضافتها بشكل منفصل إلى DC.

- تتم إضافة جميع الأجهزة المدارة إلى وحدة تيار مستمر واحدة فقط. تتم مزامنة التكوين بين وحدات التحكم في الوصول (DC) النظيرة.

- تقوم الأجهزة المدارة بإرسال السجلات إلى كل من وحدة التحكم بالمجال (DC).

- تقوم وحدات التحكم بالمجال (DC) بمزامنة أحدث الإجراءات. على سبيل المثال، إذا قمت بحذف مستخدم من DC-1، فإن النظير الآخر DC-2 لا يقوم بمزامنة تكوين المستخدم إلى DC-1. إنها تتزامن مع **إجراء الحذف** ويفقد المستخدم من كل من DC-1 و DC-2.

تمت مشاركة التكوين بشكل ثنائي الإتجاه بين النظراء

تعمل وحدات HA DC على مزامنة السياسات بشكل ثنائي الإتجاه. تتم مزامنة هذه التكوينات بشكل ثنائي الإتجاه بين النظراء. يمكنك أيضا عرض معظم هذه التكوينات بالمسار المحدد بجوارها مباشرة:

الهويات والمصادقة

- تكوين LDAP الخارجي- انتقل إلى **النظام > محلي > إدارة المستخدم > المصادقة الخارجية**
- المستخدمون (الداخليون والخارجيون)- انتقل **إلى النظام > المحليون> إدارة المستخدم> المستخدمون**

• أدوار المستخدم المخصصة- انتقل **إلى النظام > محلي > إدارة المستخدم > أدوار المستخدم**

تقارير

• قوالب التقارير- انتقل إلى **نظرة عامة > إعداد التقارير > قوالب التقارير**

السياسات القابلة للتكوين (تحت قسم السياسات)

- سياسات التحكم في الوصول، وسياسات الاقتحام، وسياسات الملفات، وسياسات طبقة الأمان (SSL)، وسياسات الوصول إلى الشبكة، وسياسات وقواعد الارتباط، وشخصيات التحكم في البيانات المتوافقة وتوصيفات حركة مرور البيانات.
- قواعد التطفل (محلي و SRU)- انتقل **إلى السياسات > التطفل> محرر القواعد > القواعد المحلية.**
- اكتشاف الشبكة وسمات المضيف وملاحظات المستخدم الخاصة باكتشاف الشبكة، بما في ذلك الملاحظات وأهمية المضيف وحذف البيئات المضيفة والتطبيقات والشبكات من خريطة الشبكة وإلغاء تنشيط نقاط الضعف أو تعديلها.
- أجهزة مخصصة لاكتشاف التطبيقات
- إتصالات LDAP في سياسات المستخدم - انتقل **إلى السياسات > المستخدمين**
- التنبيهات- انتقل إلى **السياسات> الإجراءات > التنبيهات** (أسفل الاستجابات)

معلومات الجهاز

- قواعد NAT- انتقل **إلى الأجهزة> NAT**
- قواعد VPN- انتقل **إلى الأجهزة > VPN**
- تتم مزامنة جميع معلومات الجهاز بما في ذلك الاسم ومجموعته بشكل ثنائي الإتجاه. تتم أيضا مزامنة موقع تخزين السجلات لكل جهاز بين الأجهزة النظيرة - انتقل **إلى الأجهزة > إدارة الأجهزة**
- تصنيفات مخصصة لقاعدة التطفل
- بصمات الأصابع المخصصة النشطة
- سياسة النظام والسياسة الصحية
- لوحات معلومات مخصصة، مهام سير العمل المخصصة والجداول المخصصة
- تغيير إعدادات التسوية واللقطات والتقرير
- تحديثات قاعدة SRU) Sourcefire) وقاعدة بيانات الموقع الجغرافي (GeoDB) وتحديثات قاعدة بيانات الثغرات (VDB)

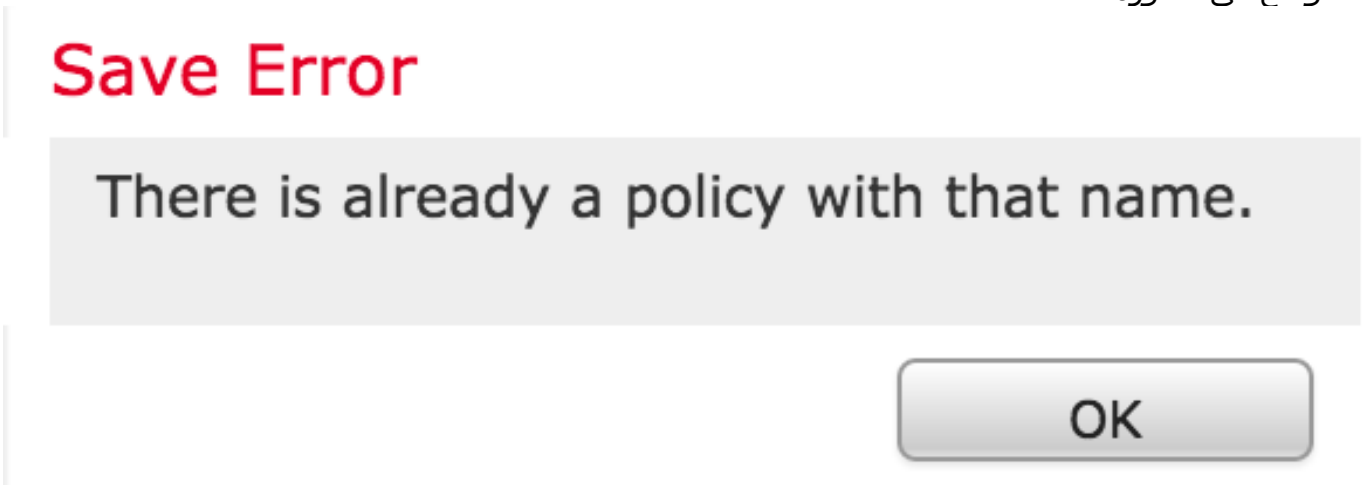
لم تتم مزامنة التكوين بين وحدات التحكم بالمجال DC

- معلومات عامل المستخدم في نهج المستخدم
- مسح NMAP
- مجموعات الاستجابة
- وحدات المعالجة النمطية
- مثيلات الإصلاح
- Estreamer وعميل إدخال المضيف
- ملفات تعريف النسخ الاحتياطي
- الجداول
- التراخيص
- التحديثات
- تنبيهات الحماية

التكوين

المتطلبات الأساسية لتكوين التوافر العالي

- يجب أن تكون الأجهزة من نفس إصدار البرامج والمكونات المادية.
- يجب أن يكون لدى الأجهزة نفس VDB المثبت.
- يجب أن تحتوي الأجهزة على نفس SRU.
- تأكد من أن لكل من مركزي الدفاع حساب مستخدم مسمى مسؤول بامتيازات المسؤول. يجب أن تستخدم هذه الحسابات نفس كلمة المرور.
- تأكد من أنه بخلاف حساب المسؤول، لا يحتوي مركزا الدفاع على حسابات مستخدمين بأسماء مستخدمين متطابقة. قم بإزالة أحد حسابات المستخدمين المضاعفة أو إعادة تسميته قبل أن تقوم بإنشاء توفر عال.
- تأكد من أن كلا الجهازين ليس لديهما أي سياسات للتحكم في الوصول بنفس الاسم. إذا كان هناك نهجان للتحكم في الوصول لهما نفس الاسم فكلاهما يتعايشان على وحدات التحكم في الوصول (DCs). ومع ذلك، لا يمكن إقرانهم بأي جهاز.بمجرد حفظ هذا النهج بعد إضافة جهاز هدف، يتم رفض هذا التكوين مع حدوث خطأ كما هو موضح في الصورة:



- ويجب أن يكون لكل من مركزي الدفاع حق الوصول إلى الإنترنت.

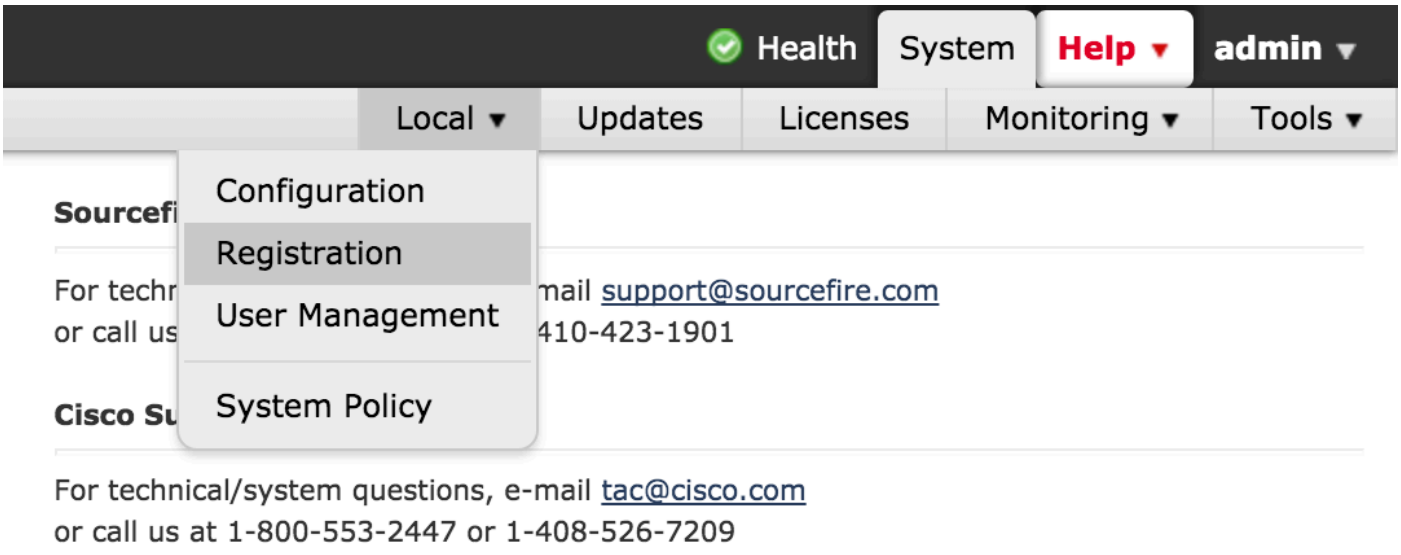
تكوين التوافر العالي

هذه هي 8 خطوات لتكوين التوفر العالي.

الخطوة 1. تأكد من أن إصدار البرامج والأجهزة بالإضافة إلى إصدار VDB وإصدار تحديث القاعدة هي نفسها.

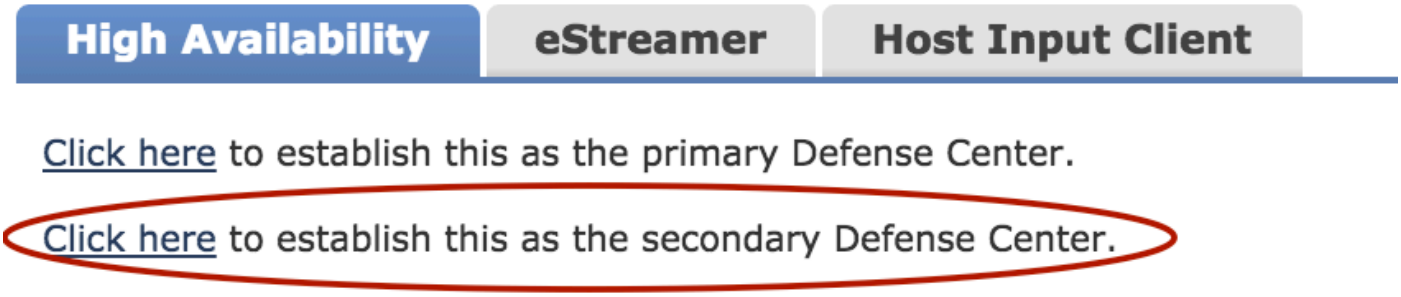
Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build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

الخطوة 2. لتجعل جهازك ثانوي، انتقل إلى **النظام > محلي > التسجيل**، كما هو موضح في الصورة. تأكد من عدم وجود تكوين على وحدة التحكم بالمجال هذه.

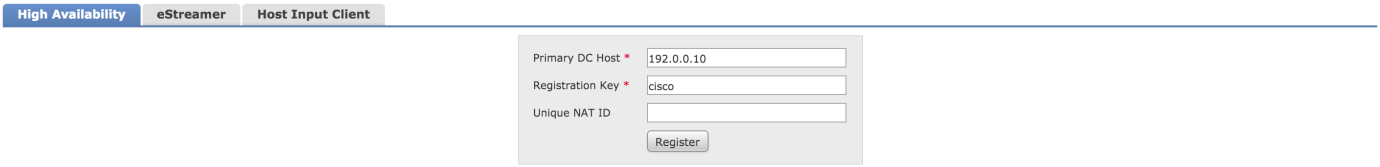


الخطوة 3. تحت علامة التبويب **توفر عال** انقر فوق **انقر هنا لإنشاء هذا كمركز دفاع ثانوي**، كما هو موضح في

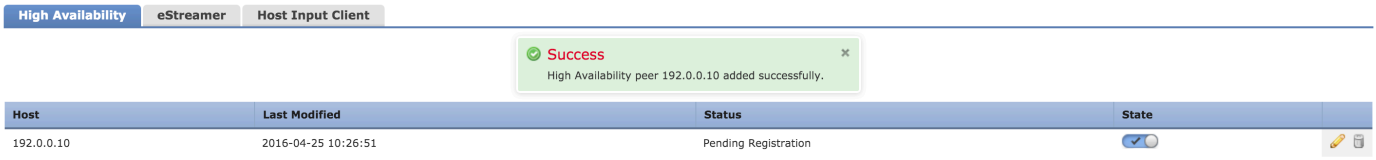
الصورة:



الخطوة 4. وأنت تكمل الخطوة 3، يتم عرض صفحة كما هو موضح في الصورة. قم بإضافة عنوان IP الخاص بوحدة التحكم بالمجال (DC) الأساسية ومفتاح المرور. ضمنت أن أنت تضيف معرف nat فريد للأجهزة، أي يكون وراء شبكة عنوان ترجمة.



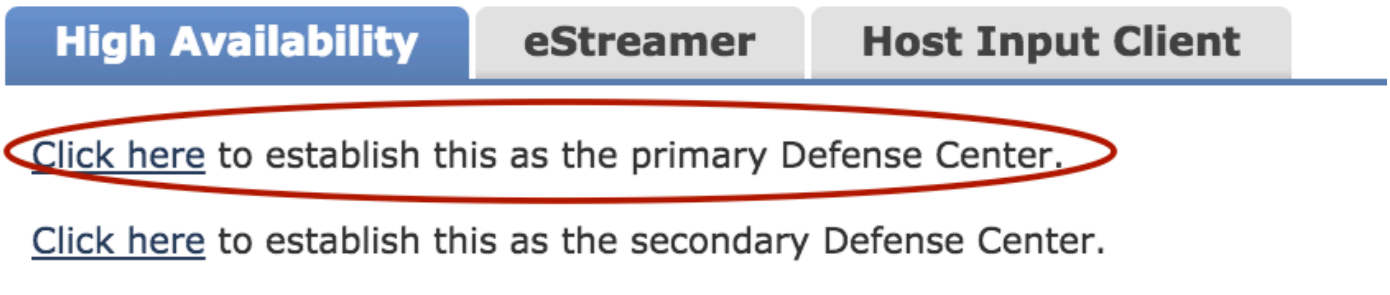
الخطوة 5. بعد التحقق من عنوان IP، إذا تم النقر بشكل صحيح على **التسجيل**. سترى صفحة كما هو موضح في الصورة:



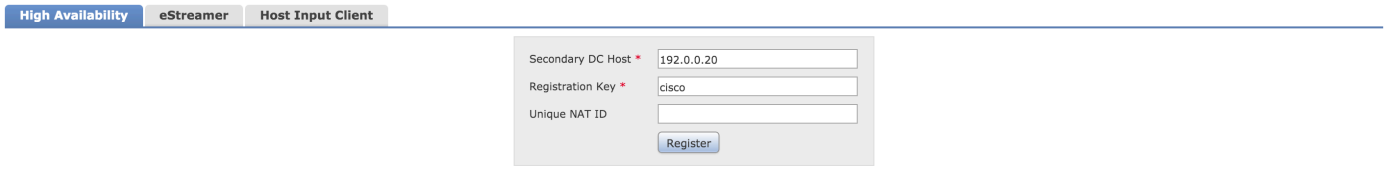
وهذا يعني أنه تم تكوين HA على DC الثانوي وتحتاج إلى تكوينه على DC الأساسي.

الخطوة 6. قم بتسجيل الدخول إلى الجهاز الذي ترغب في تكوينه كتيار DC أساسي. انتقل إلى **النظام > المحلي > التسجيل.**

تحت علامة التبويب **الإتاحة العالية** انقر فوق **انقر هنا لإضافة مركز الدفاع الرئيسي**، كما هو موضح في الصورة:

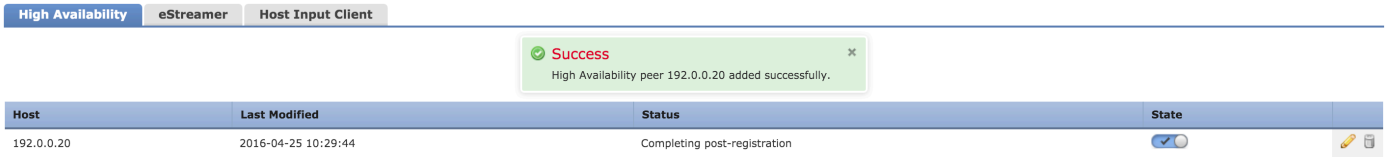


الخطوة 7. بعد أن تكمل الخطوة 6، يتم عرض صفحة كما هو موضح في الصورة:



قم بإضافة عنوان IP الثانوي للتيار المستمر. قم بتوفير مفتاح التسجيل نفسه ومعرف NAT الذي تم توفيره أثناء تكوين وحدة التحكم بالمجال الثانوية.

الخطوة 8. بعد التحقق من تفاصيل IP، انقر على **التسجيل**. بمجرد اكتمال التسجيل، تظهر صفحة العمل كما هو موضح في الصورة:



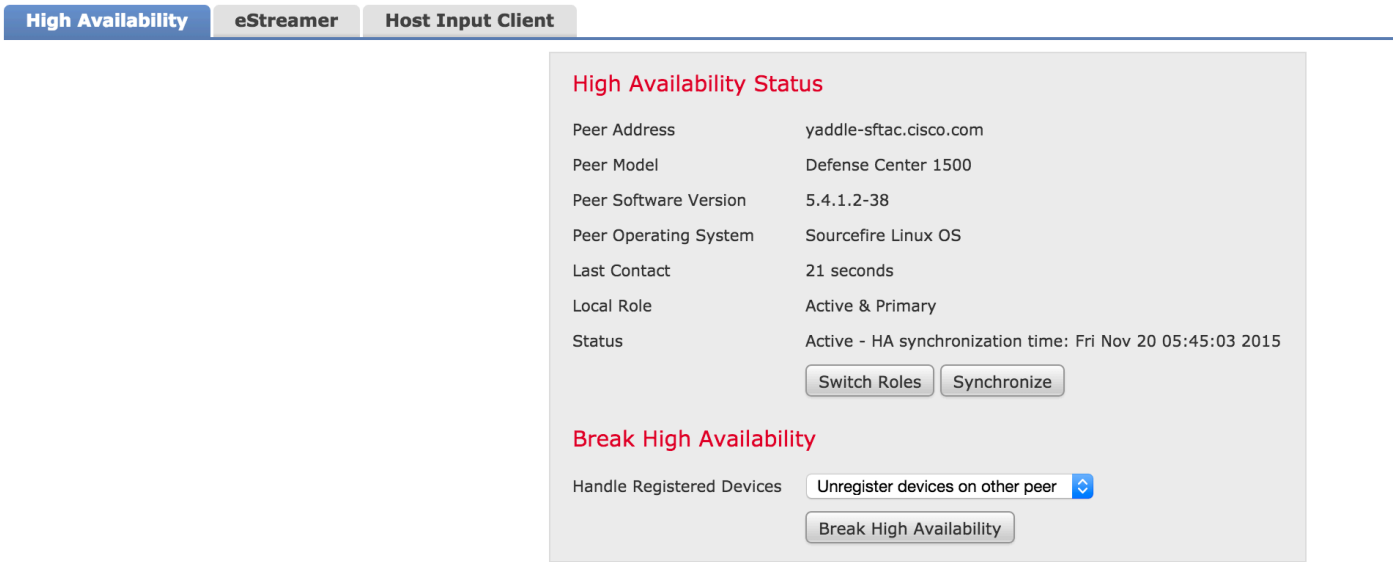
بعد 5 إلى 10 دقائق يتم إكمال تهيئة HA ومزامنتها.

يستغرق الأمر ما بين 5 إلى 10 دقائق لإكمال تهيئة HA ومزامنتها

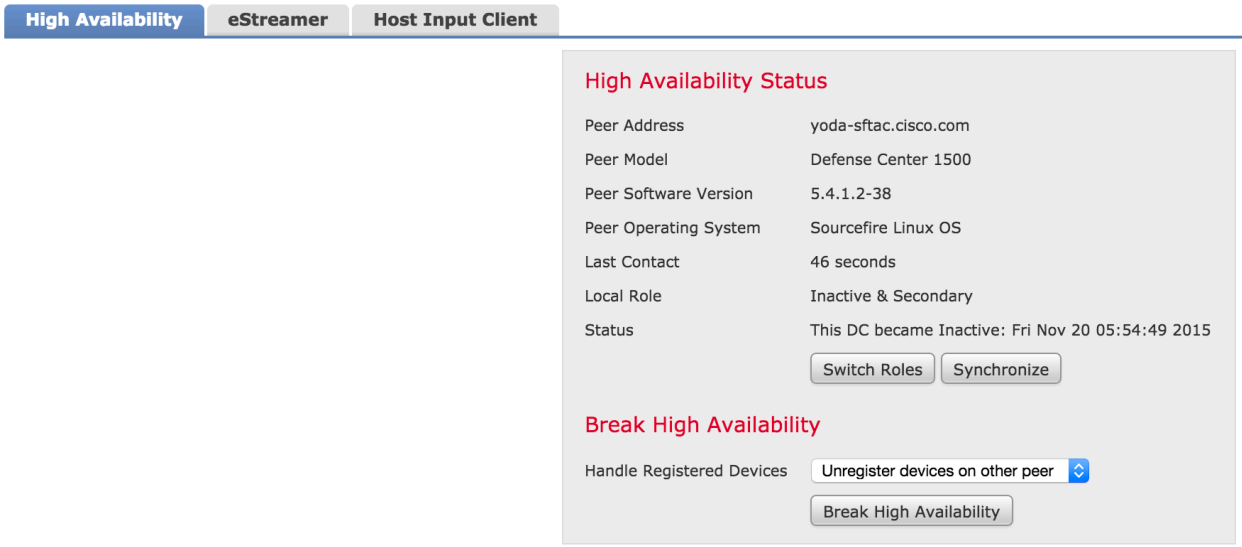
التحقق من الصحة

التهيئة خطوة بخطوة للتحقق من تكوين وحدة التحكم بالمجال (DC) بشكل صحيح للحصول على توفر فائق.

الخطوة 1. انتقل إلى **النظام >محلي >تسجيل** على الجهاز الأساسي كما هو موضح في الصورة:



الخطوة 2. انتقل إلى **النظام >محلي >تسجيل** على الجهاز الثانوي كما هو موضح في الصورة:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم خطوات أستكشاف الأخطاء وإصلاحها الأساسية للحصول على توفر فائق.

- تأكد من أن كل من وحدة التحكم بالمجال (DC) تستمع إلى منفذ TCP 8305، نظرا لأن HA يستخدم هذا المنفذ لمزامنة المعلومات ودقات القلب.
- تأكد من أن منفذ TCP 8305 غير محظور في الشبكة أو بواسطة أي أجهزة وسيطة.
- يفشل إنشاء HA في حالة وجود إدخال قديم لجهاز نظير سابق تتم إزالته أو إستبداله. يوفر جدول EM_PEERS المزيد من المعلومات حول هذه الأجهزة النظيرة.

معلومات ذات صلة

- تكوين المكدس على أجهزة سلسلة Cisco Firepower 8000
- دليل مستخدم نظام FireSIGHT 5.4.1
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).