يدو أن أحداث الاتصال تختفي من مركز إدارة FireSIGHT

المحتويات

المقدمة

يوضح هذا المستند كيفية تحديد السبب الجذري واستكشاف المشكلة وإصلاحها عند إختفاء أحداث الاتصال من مركز إدارة FireSIGHT بعد تشغيل النظام لعدة أيام. قد يحدث ذلك بسبب إعدادات تكوين مركز الإدارة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بمركز إدارة FireSIGHT.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- FireSIGHT Management Center
- الإصدار 5.2 من البرنامج أو إصدار أحدث

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.

استكشاف الأخطاء وإصلاحها

الخطوة 1: تحديد عدد الأحداث المخزنة

لتحديد عدد أحداث الاتصال التي يتم تخزينها على مركز إدارة FireSIGHT،

1. أختر **تحليل > إتصالات > عرض جدول لأحداث الاتصال**.
2. قم بتوسيع الإطار الزمني إلى نطاق واسع يشمل جميع الأحداث الحالية، على سبيل المثال، 12 شهرا.
3. لاحظ العدد الإجمالي للصفوف في أسفل الصفحة. انقر الصفحة الأخيرة ولاحظ الطابع الزمني لآخر حدث اتصال متاح.

تعطيك هذه المعلومات فكرة عن عدد وفترة استمرارك في أحداث الاتصال مع التكوين الحالي لديك.

الخطوة 2: تحديد خيار التسجيل

راجع الاتصالات التي يتم تسجيلها، وأين يتم تسجيل الاتصالات في التدفق. يجب تسجيل الاتصالات بما يتوافق مع إحتياجات الأمان والتوافق الخاصة بمؤسستك. إذا كان هدفك هو الحد من عدد الأحداث التي تقوم بإنشائها، قم فقط بتمكين التسجيل للقواعد الضرورية للتحليل. ومع ذلك، إذا كنت تريد طريقة عرض واسعة لحركة مرور الشبكة، فيمكنك تمكين التسجيل لقواعد التحكم في الوصول الإضافية أو للإجراء الافتراضي. يمكنك تعطيل تسجيل الاتصال لحركة المرور غير الضرورية للمساعدة في الاحتفاظ بأحداث الاتصال لفترة زمنية أطول.

تلميح: لتحسين الأداء، توصيك Cisco بتسجيل بداية الاتصال أو نهايته، وليس كليهما.

ملاحظة: بالنسبة لاتصال واحد، يحتوي حدث نهاية الاتصال على جميع المعلومات في حدث بدء الاتصال وكذلك المعلومات التي تم جمعها خلال مدة الدورة. بالنسبة لقواعد الثقة والسماح، يوصى باستخدام نهاية الاتصال.

يشرح هذا المخطط خيارات التسجيل المختلفة المتوفرة لكل إجراء قاعدة:

إجراء القاعدة أو خيار التسجيل	تسجيل عند البداية	تسجيل عند الانتهاء
إستئمانا	X	X
الإجراء الافتراضي: الثقة سماح		
الإجراء الافتراضي: التطفل	X	X
الإجراء الافتراضي: الاكتشاف		
جهاز العرض كتلة		X (مطلوب)
حظر مع إعادة تعيين	X	
إجراء التفكيك: الحظر كتلة تفاعلية		
كتلة تفاعلية مع إعادة تعيين	X	س (إذا تم تجاوزه)
الإستخبارات الأمنية	X	

الخطوة 3: ضبط حجم قاعدة بيانات الاتصال

تعتمد أحداث الاتصال على الإعداد Maximum Connection Events في نهج النظام. لتغيير الإعداد:

1. أختر **نظام > محلي > سياسة النظام**.

2. انقر على أيقونة *القلم الرصاص* لتحرير السياسة المطبقة حاليا.
3. أختر **قاعدة بيانات > قاعدة بيانات الاتصال > الحد الأقصى لأحداث الاتصال**.
4. تغيير قيمة **الحد الأقصى لأحداث الاتصال**.
5. انقر فوق **حفظ النهج والخروج**، ثم **تطبيق** النهج على الأجهزة.

يعتمد الحد الأقصى لحجم أحداث الاتصال التي يمكن تخزينها على نموذج مركز الإدارة:

ملاحظة: تتم مشاركة الحد الأقصى للحدث بين أحداث الاتصال وأحداث إستخبارات الأمان؛ ولا يمكن أن يتجاوز مجموع الحدود القصوى التي تم تكوينها للحادثين الحد الأقصى للحدث.

نموذج مركز الإدارة	الحد الأقصى لعدد الأحداث
FS750 و DC750	50 مليون
FS1500 و DC1500	مائة مليون
الطراز FS2000	300 مليون
FS3500 و DC3500	500 مليون
الطراز FS4000	1 بليون
الجهاز الظاهري	10 ملايين

تحذير: يمكن أن يكون لزيادة حدود قاعدة البيانات تأثير ضار على الأداء على الجهاز. من أجل تحسين الأداء، يجب عليك أن تضع حدود الحدث بحسب عدد الأحداث التي تعمل معها بشكل منتظم.

بالنسبة للودجات التي يتم فيها عرض عدد الأحداث عبر نطاق زمني، قد لا يعكس العدد الإجمالي للأحداث عدد الأحداث التي تتوفر بيانات تفصيلية عنها في عارض الأحداث. يحدث ذلك لأن النظام يقوم أحيانا بتقليم تفاصيل الأحداث القديمة لإدارة إستخدام مساحة القرص. من أجل تقليل تكرار تنقيح تفاصيل الحدث إلى الحد الأدنى، يمكنك ضبط تسجيل الأحداث لتسجل فقط تلك الأحداث الأكثر أهمية لنشرك.

معلومات ذات صلة

- تكوين حدود حدث قاعدة البيانات
- 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).