تكوين أحداث أمان SLF و SQLF في التحليلات الآمنة

المحتويات

المقدمة

معلومات أساسية

الضبط/التكوين

الحل

المقدمة

يصف هذا المستند معلمتين يمكن إستخدامهما لمعايرة أحداث أمان التدفق الطويل (SLF) المشتبه به والتشكيك في وجود أحداث أمان التدفق الطويل الهادئ (SQLF).

معلومات أساسية

يعد حدث التدفق الطويل المشكوك فيه نوعا محددا من أحداث الأمان التي تم إنشاؤها بواسطة "تحليلات الأمان" والتي تم تصميمها لاكتشاف المحادثات الأطول من العادية بين الأجهزة المضيفة. هناك نوعان مختلفان من حدث Suspect Long Flow؛ اشتباه في التدفق الطويل والتساهل في طول التدفق.

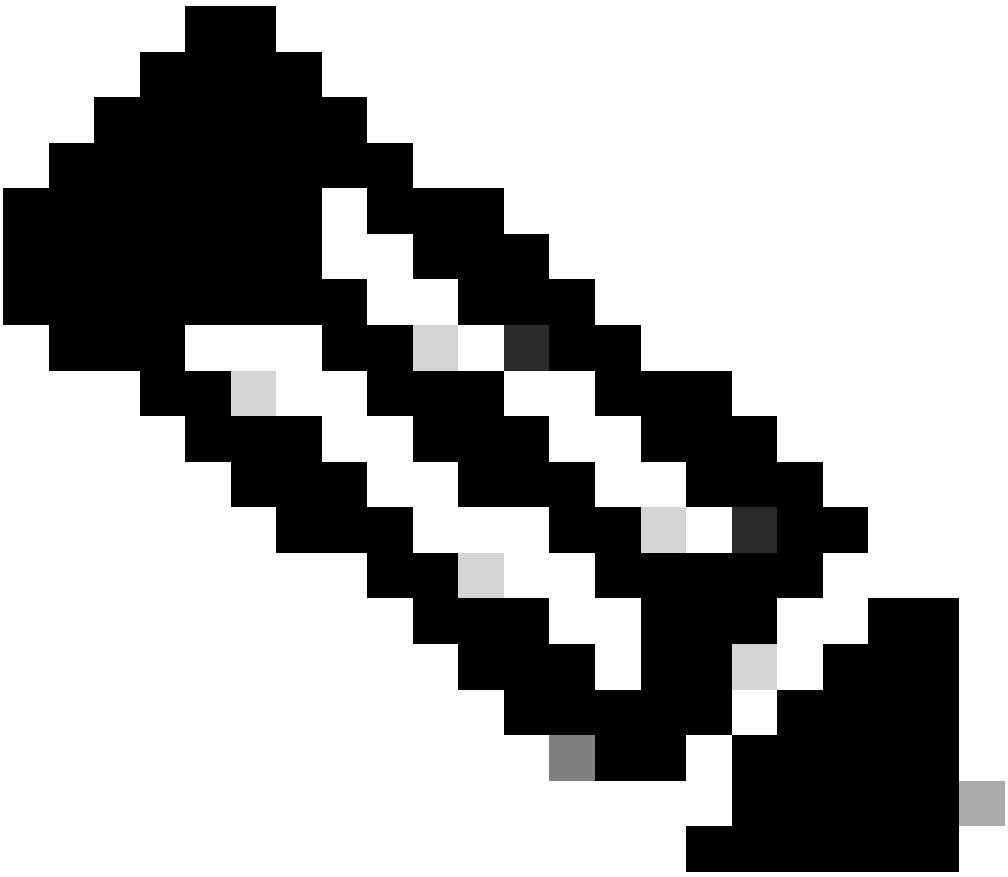
ضع في اعتبارك توصيل جهاز الكمبيوتر المحمول بجهاز الكمبيوتر المنزلي لديك من خلال شبكة خاصة ظاهرية (VPN) سرية لمدة 3 أيام، ولكن عادة ال يحمل جهاز الكمبيوتر المنزلي أو الكمبيوتر المحمول أية إتصالات تدفق طويلة. يقوم مجمع التدفق بكشف هذا الشذوذ وتشغيل حدث أمان وفقا لمقدار حركة المرور التي تم تمريرها ومدة التدفق. الغرض من هذه الأحداث هو تحديد التدفقات التي يتم تشغيلها لمدة طويلة والتدفقات التي يتم تشغيلها لمدة طويلة والتي تقوم بتمرير الحد الأدنى من حركة المرور.

الضبط/التكوين

هناك بشكل أساسي 2 من معلمات تكوين مجمع التدفق المسؤولة عن التحكم في سلوك هذين الحدثين.

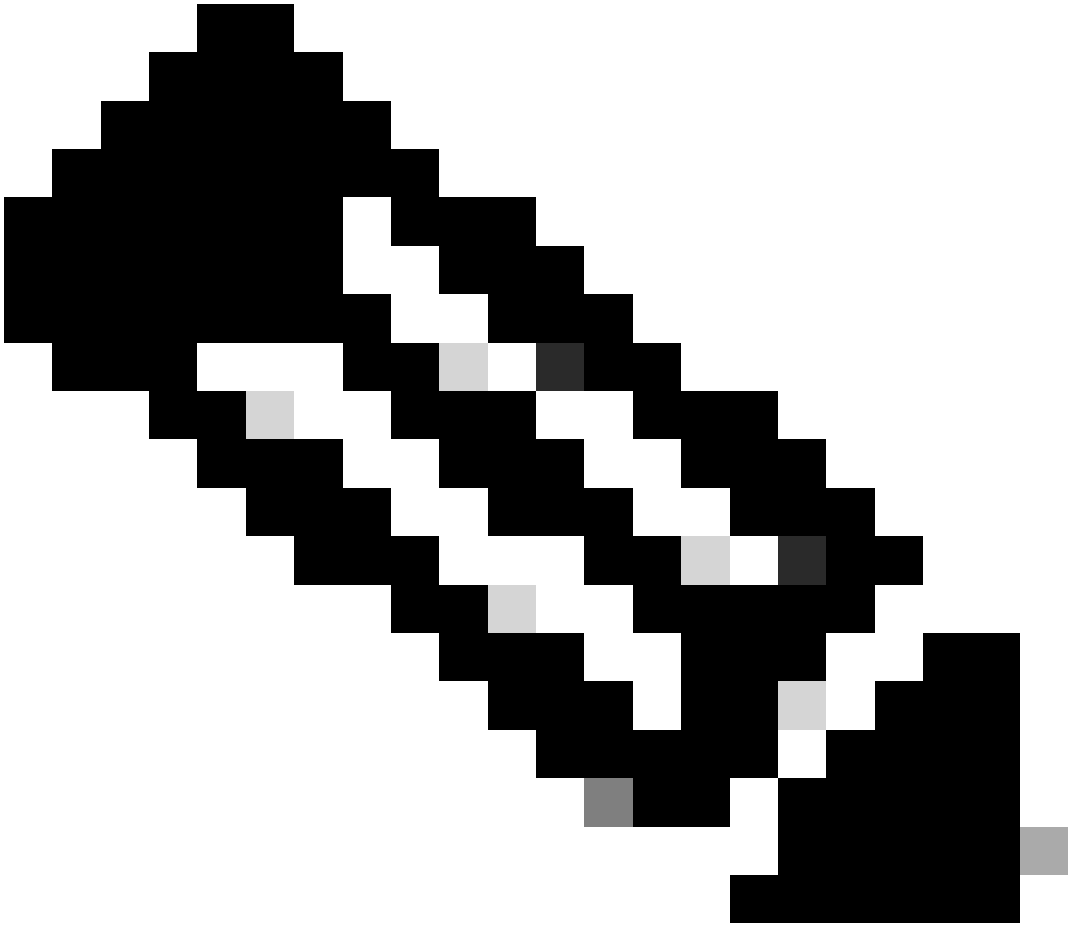
يمكن ضبط هذه الإعدادات عن طريق الوصول إلى Configure (تكوين) > Flow Collectors (أدوات تجميع التدفق) > Advanced Page في WebUI (واجهة مستخدم الويب) الخاصة بجهاز الإدارة.

- تتحكم الثواني المطلوبة لتأهيل تدفق ما إعداد مدة طويلة في سلوك حدث التدفق الطويل المشتبه فيه.



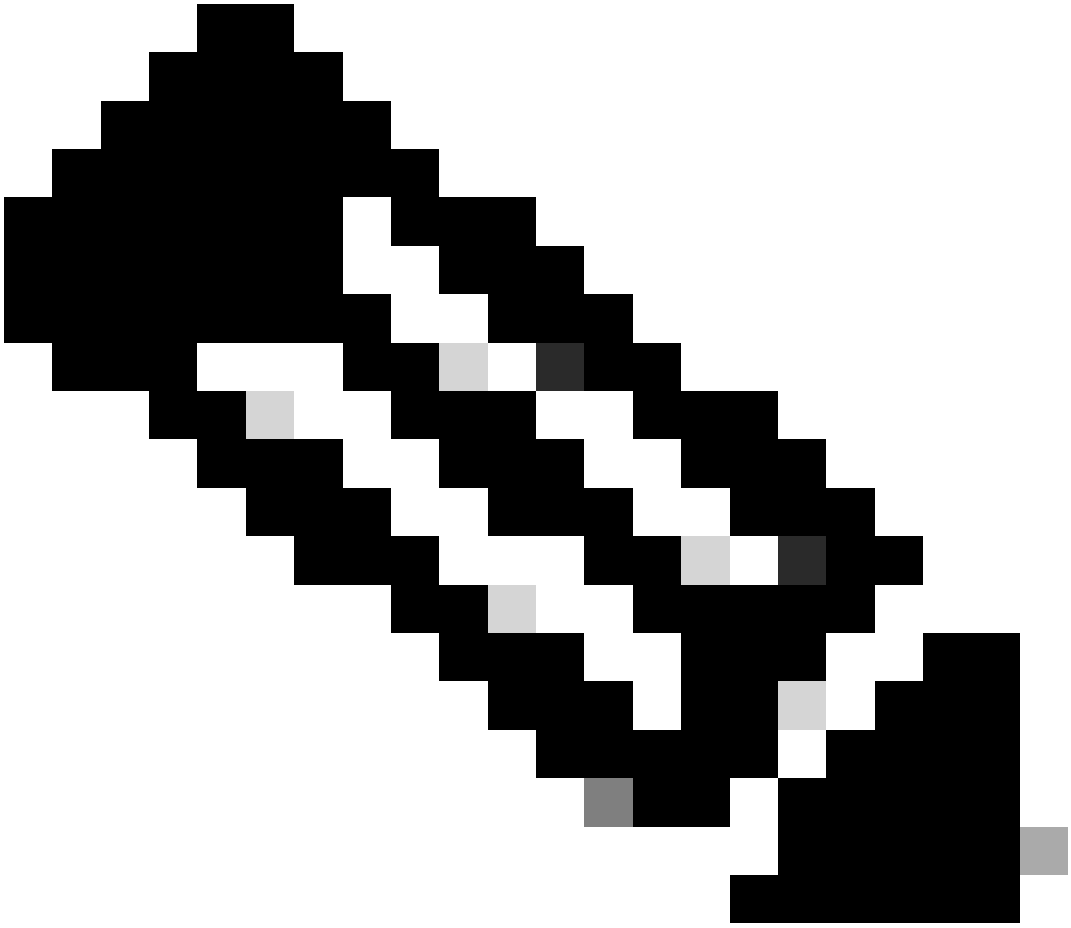
ملاحظة: يقوم خيار التكوين هذا في WebUI بتعيين المعلمة long_flow_duration في ملف تكوين أدوات تجميع التدفق lc_threshold.txt.

- الثواني المطلوبة لتأهيل التدفق حيث تتحكم إعدادات التدفق الطويل الهادئ المشتبه بها في سلوك حدث Quiet Long Flow المشتبه فيه.



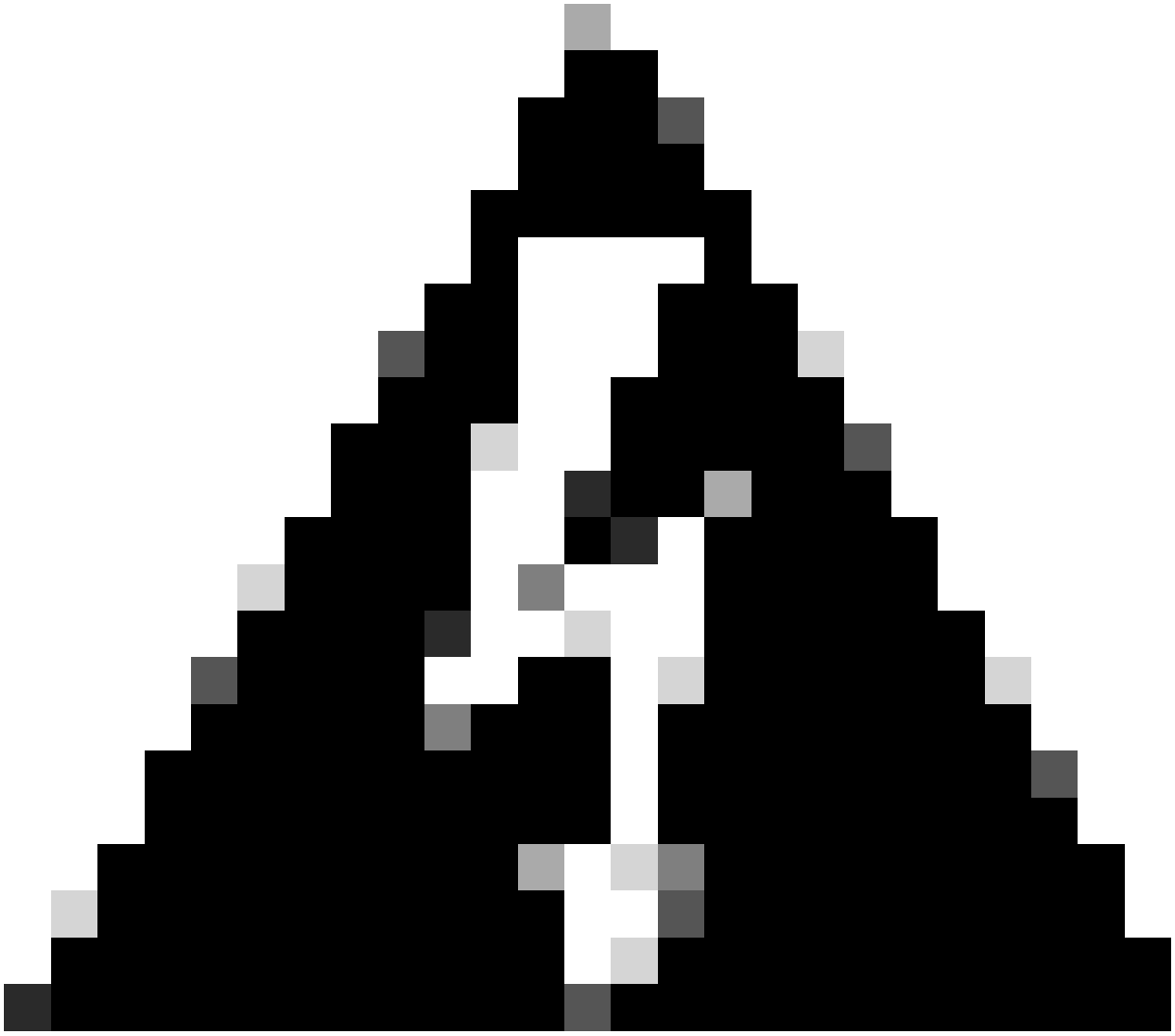
ملاحظة: يقوم خيار التكوين هذا في WebUI بتعيين المعلمة quiet_long_flow_duration في ملف تكوين أدوات تجميع التدفق lc_threshold.txt.

القيمة الافتراضية لكل من العداد هي 32400 ثانية (9 ساعات).



ملاحظة: فيما يتعلق بتغيير هذه العدادات، CDET ذات الصلة:

معرف تصحيح الأخطاء من Cisco CSCwm05128



تحذير: يؤثر هذا فقط على الإصدار 7.5.1 وأ الإصدارات السابقة.

وهذا العيب يفرض على المشتبه به أن يستمر في التدفق لفترة طويلة من الزمن حتى ولو اشتبه في ذلك. وهذا يعني أنك إذا قمت بتغيير الثواني المطلوبة لتأهيل التدفق كتدفق هادئ مشتبه به إلى مدة أقصر من الثواني المطلوبة لتأهيل التدفق كإعداد مدة طويلة، فإن النتائج غير المتوقعة تكون محتملة.

إن يغير أنت واحد أو كل من هذا متقدم عملية إعداد، وهو يستطيع سبب كشف التدفقات طويلة أن يفشل.

بما أن التدفق الطويل الهادئ بموجب التعريف يجب أن يكون أيضا تدفق طويل، فإن المنطق في المعالجة السليمة لهذين الإعدادين هو أولا أن يكون التدفق يتجاوز متطلبات التدفق الطويل قبل الاختبار ليكون تدفق طويل هادئ.

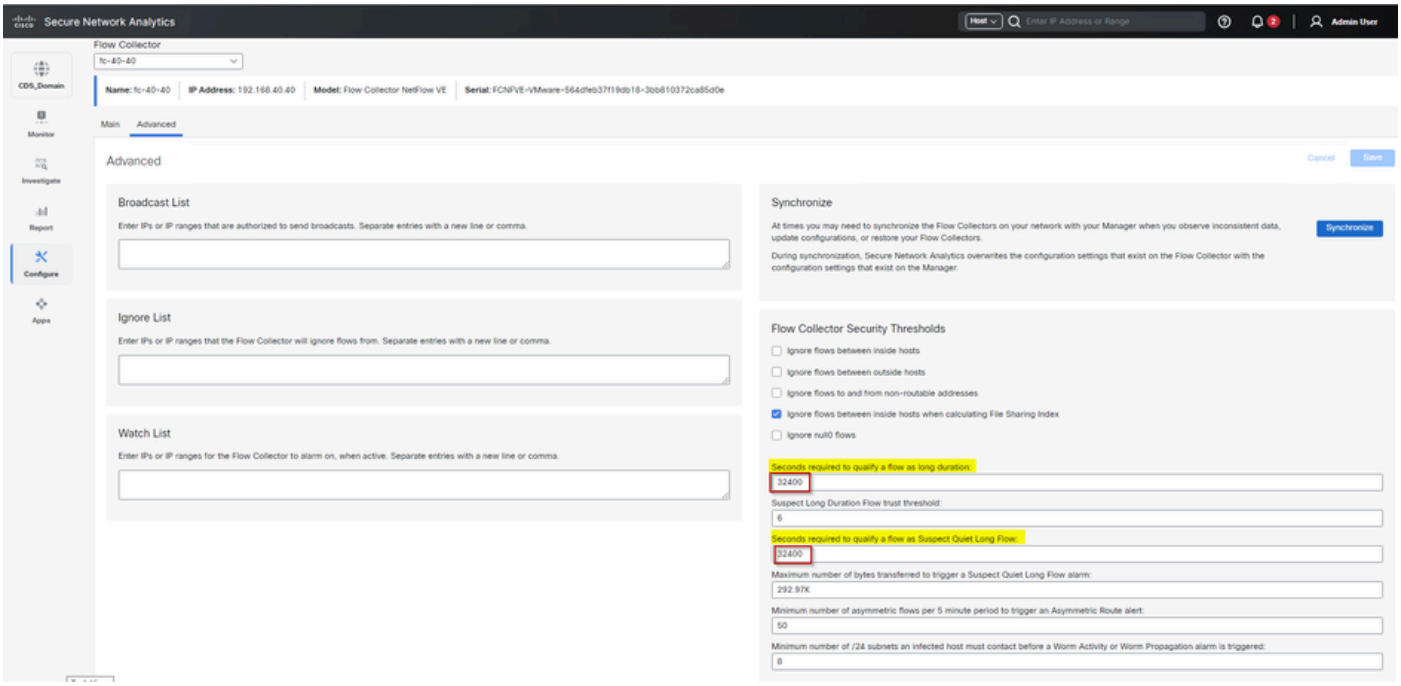
على سبيل المثال، إذا تم ترك LONG_FLOW_DURATION عند القيمة الافتراضية 9 ساعات وتم تعيين QUIET_LONG_FLOW_DURATION على قيمة أقل مثل 8 ساعات، فلن يقوم المحرك برفع حدث تدفق هادئ لفترة طويلة حتى يصبح التدفق طويل بما لا يقل عن 9

ساعات.

بدلا من ذلك، إذا تم ترك LONG_FLOW_DURATION عند القيمة الافتراضية 9 ساعات وتم تعيين QUIET_LONG_FLOW_DURATION على 10 ساعات، فإن هذا التكوين يقوم بشكل فعال بتعطيل حدث التدفق الهادئ طويل المدة (ما لم يكن التدفق عبارة عن تصدير واحد له مدة > QUIET_LONG_FLOW_DURATION تبلغ 10 ساعات.

الحل

يجب تعيين كل من هذه الإعدادات المتقدمة إلى نفس القيمة المطلوبة أو يجب أن يكون quiet_long_flow_duration دائما >= long_flow_duration.



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).