

تارم ددع ضرعل FireSIGHT ةرادإ زكرم نيوكت لوصلو ةدعاق لكل لوصلو

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)

المقدمة

يوضح هذا المستند كيفية تكوين صفحة عارض أحداث/سير عمل مخصصة لعرض عدد مرات الاتصال لكل اسم قاعدة وصول. يعرض التكوين مثالا أساسيا لحل اسم القاعدة المقترن بأعداد عمليات الوصول وكيفية إضافة حقول إضافية إذا لزم الأمر.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة تقنية FirePOWER
- معرفة التنقل الأساسي داخل مركز إدارة FireSIGHT

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

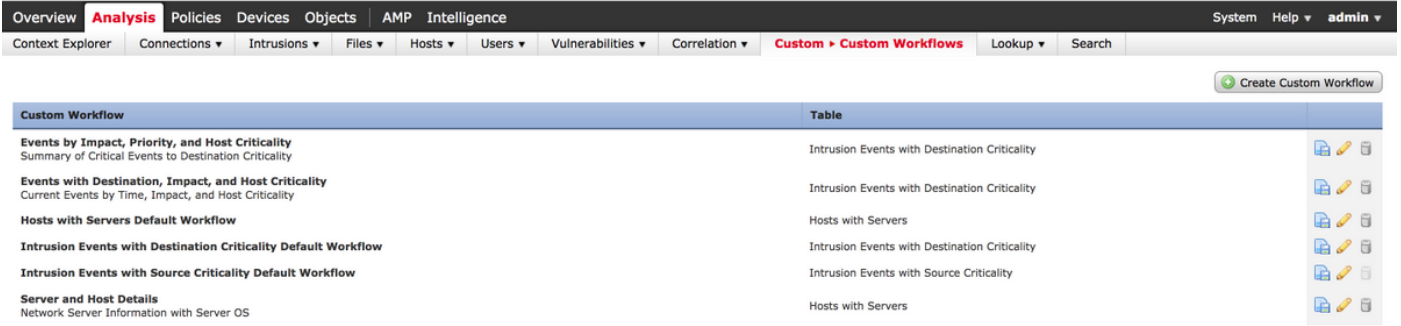
- مركز إدارة Firepower الإصدار x.6.1 والإصدارات الأحدث
 - قابل للتطبيق على أجهزة استشعار التهديد المدارة Defense/Firepower
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

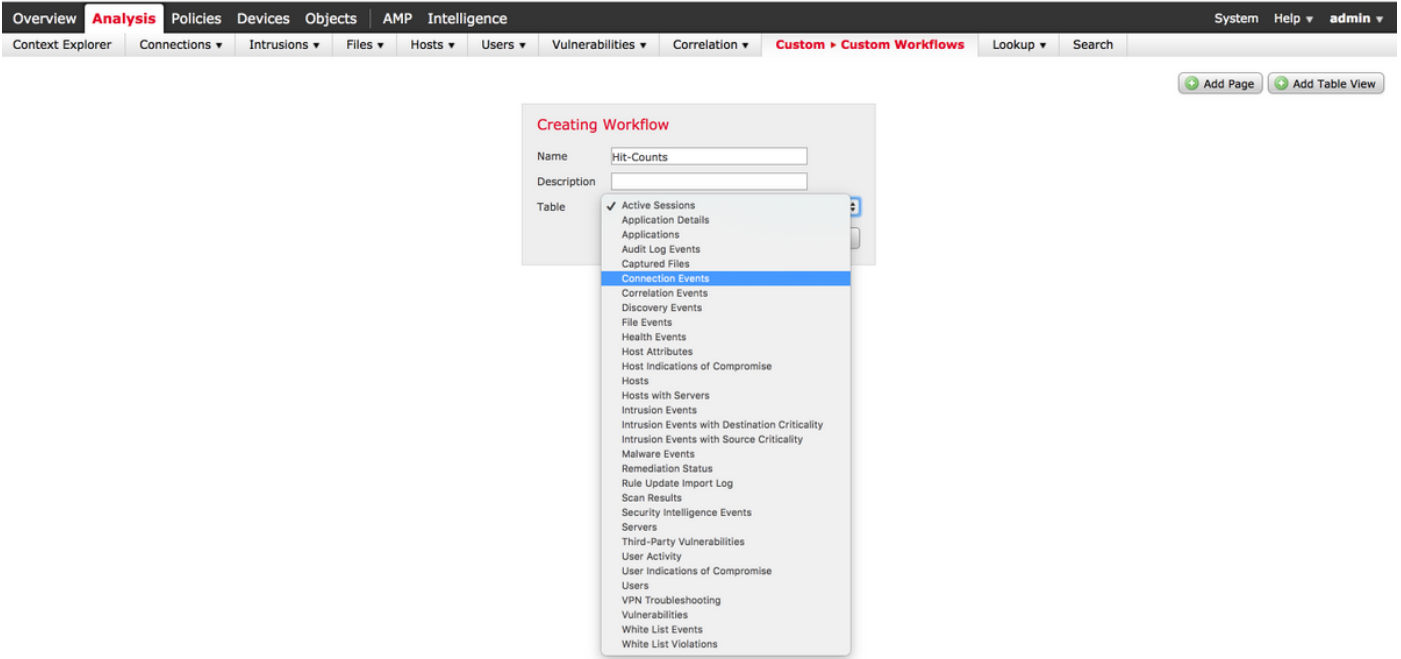
التكوينات

الخطوة 1. تسجيل الدخول إلى FireSIGHT Management Center بامتيازات المسؤول.

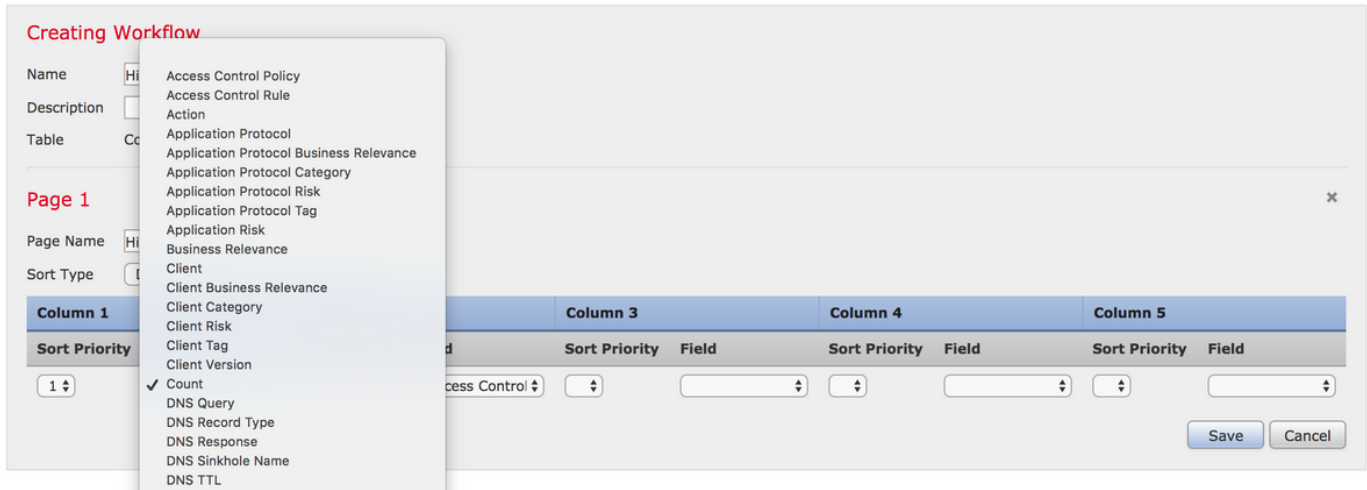
بمجرد نجاح تسجيل الدخول، انتقل إلى **Analysis (التحليل) < Custom (المخصص) < Custom Workflow (مهام سير العمل المخصصة)**، كما هو موضح في الصورة:



الخطوة 2. انقر فوق إنشاء سير عمل مخصص واختار المعلمات كما هو موضح في الصورة:



الخطوة 3. حدد حقل الجدول كأحداث اتصال وأدخل اسم سير عمل، ثم انقر على حفظ. بمجرد حفظ سير العمل، انقر على إضافة صفحة كما هو موضح في الصورة:



ملاحظة: يجب أن يكون العمود الأول هو Count، ثم في العمود الإضافي يمكنك الاختيار من بين الحقول المتاحة من القائمة المنسدلة. في هذه الحالة، يكون العمود الأول هو Count والعمود الثاني هو "قاعدة التحكم بالوصول".

الخطوة 4. بمجرد إضافة صفحة سير العمل، انقر على حفظ.

لعرض عدد مرات الوصول، انتقل إلى **Analysis (التحليل) > Events > Connections (الاتصالات)** وانقر فوق **Switch Workflow**، كما هو موضح في الصورة:

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer **Connections > Events** Intrusions Files Hosts Users Vulnerabilities Correlation

Connection Events ×

Connection Events > Table View of Connection Events

Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone
	Allow		10.1.1.5		52.39.210.199	USA	
	Allow		10.1.1.5		10.76.77.50		
	Allow		10.1.1.5		10.76.77.50		
	Allow		10.1.1.5		52.39.210.199	USA	
	Allow		10.1.1.5		10.106.38.75		
	Allow		10.1.1.5		10.106.38.75		
2017-07-19 08:47:13	Allow		10.1.1.5		10.76.77.50		
2017-07-19 08:47:08	Allow		10.1.1.5		10.76.77.50		
2017-07-19 08:47:08	Allow		10.1.1.5		172.217.7.238	USA	

الخطوة 5. من القائمة المنسدلة، اختر سير العمل المخصص الذي أنشأته (في هذه الحالة عدد مرات الوصول)، كما هو موضح في الصورة:

No Search Constraints [\(Edit Search\)](#)

Jump to...	Count	Access Control Rule
↓ □	66	Default-Allow

Displaying row 1 of 1 rows | << Page 1 of 1 >>

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل