مركز إدارة Firepower: عدادات الدخول الخاصة بنهج التحكم بالوصول للعرض

المحتويات

المقدمة

المتطلبات الأساسية

يصف هذا المستند التعليمات الخاصة بإنشاء **عمليات سير عمل مخصصة** على مركز إدارة FirePOWER (FMC) الذي يسمح للنظام بعرض عدادات الوصول الخاصة بسياسة التحكم في الوصول (ACP) على أساس عمومي وكل قاعدة. يعد هذا الأمر مفيدا لاستكشاف أخطاء تدفق حركة المرور وإصلاحها إذا ما كانت تتطابق مع القاعدة الصحيحة. كما أنه من المفيد الحصول على معلومات حول الاستخدام العام لقواعد التحكم في الوصول، على سبيل المثال، قواعد التحكم في الوصول التي لا يوجد بها أي نتائج لمدة زمنية طويلة إشارة إلى أن القاعدة لم تعد مطلوبة ويمكن إزالتها بأمان من النظام.

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

- مركز إدارة Virtual Firepower (FMC) - إصدار البرنامج 6.1.0.1 (بنية 53)
- الدفاع ضد تهديد 4150 Firepower (FTD) - نسخة البرنامج 6.1.0.1 (Build 53)

ملاحظة: لا تنطبق المعلومات الموضحة في هذا المستند على مدير أجهزة FirePOWER (FDM).

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

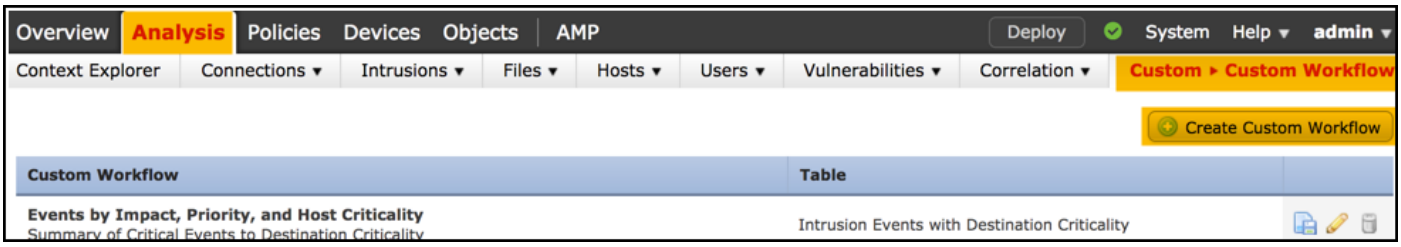
هذا وثيقة يستطيع أيضا كنت استعملت مع هذا جهاز وبرمجية صيغة:

- مركز إدارة Firepower (FMC) - إصدار البرنامج x.6.0 والإصدارات الأحدث

التكوين

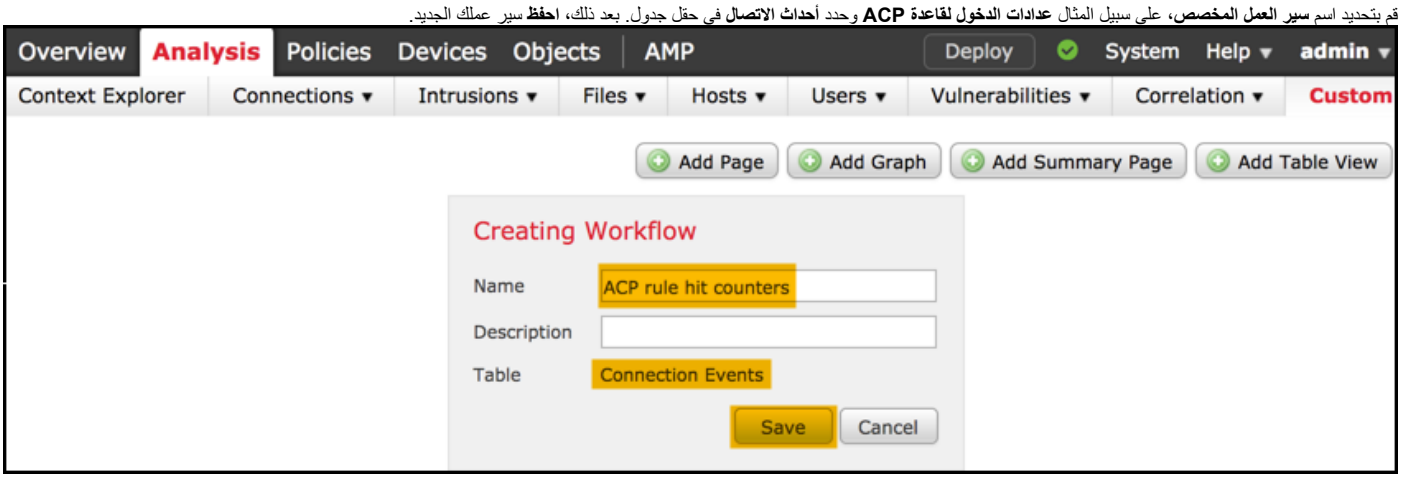
الخطوة 1

لإنشاء سير عمل مخصص، انتقل إلى **تحليل > مخصص > مهام سير عمل مخصصة > إنشاء سير عمل مخصص:**



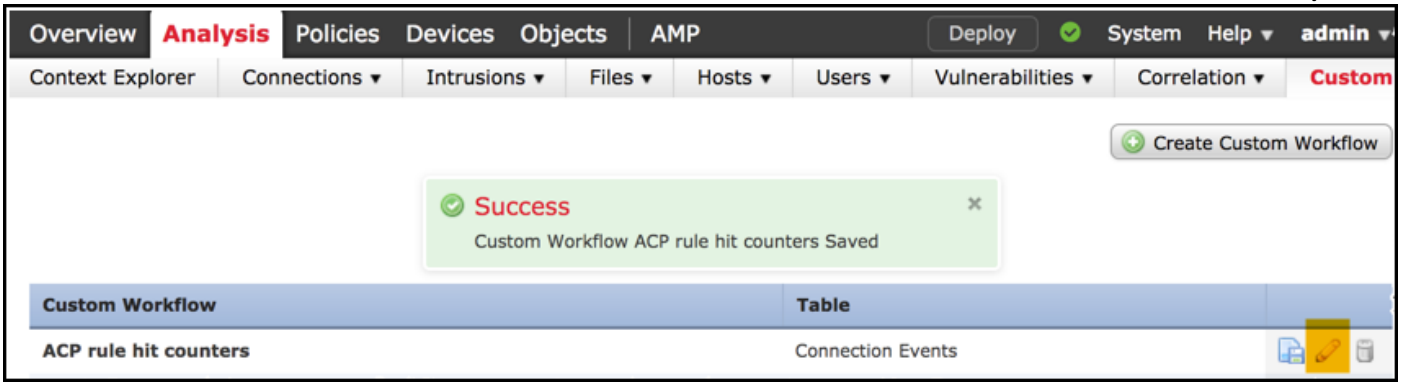
الخطوة 2

قم بتحديد اسم **سير العمل المخصص**، على سبيل المثال **عدادات الدخول لقاعدة ACP** وحدد **أحداث الاتصال** في حقل جدول. بعد ذلك، **احفظ** سير عملك الجديد.



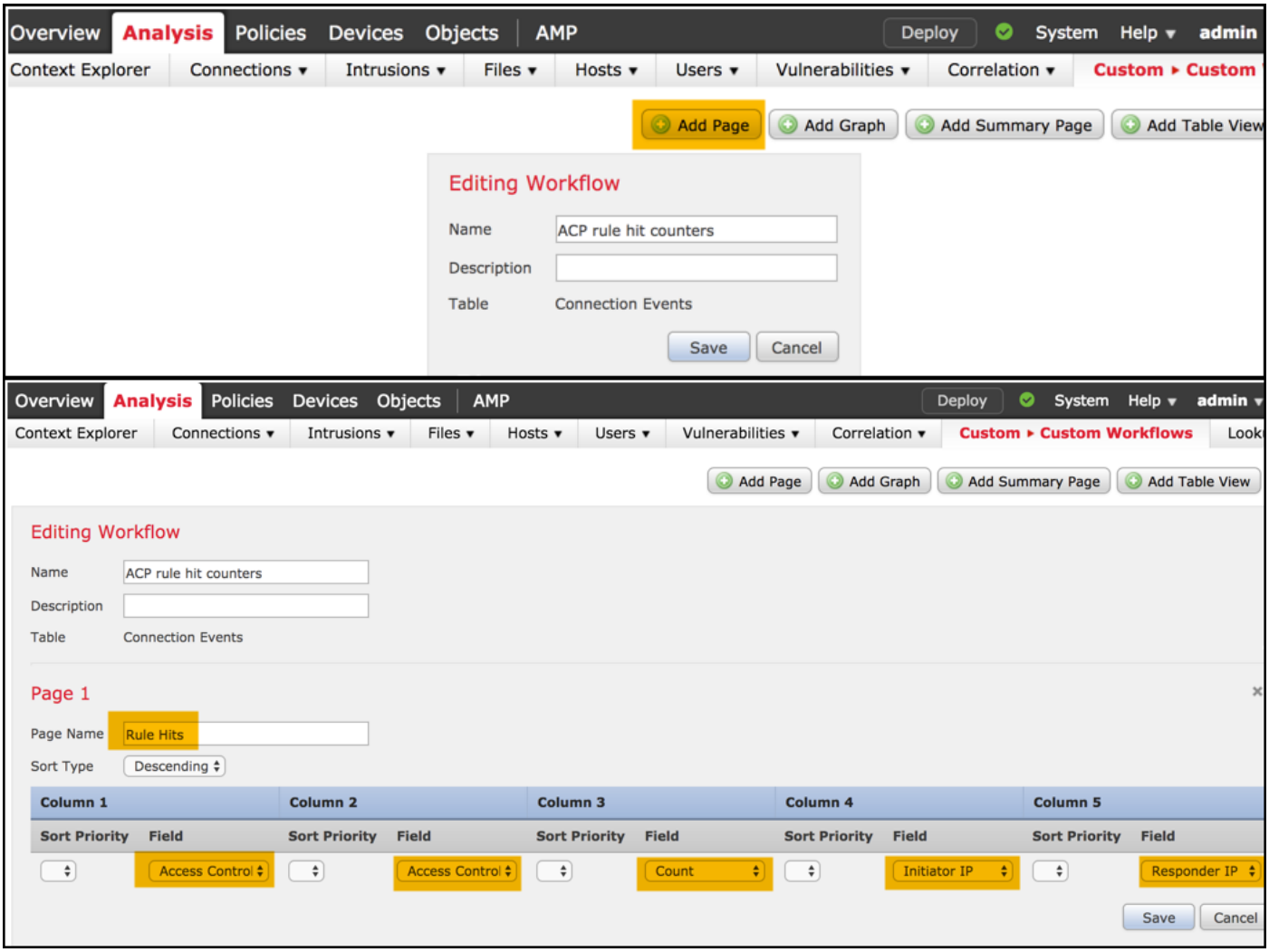
3

. /



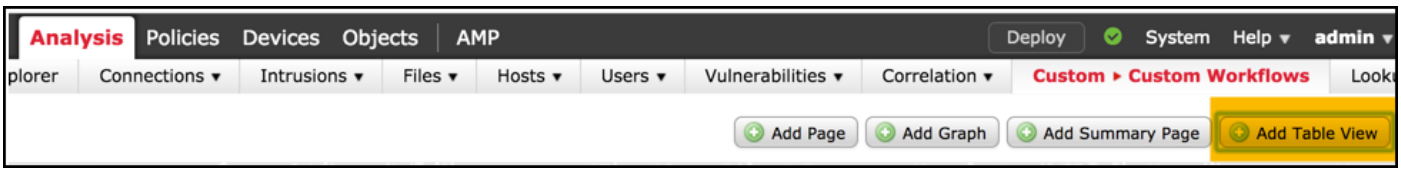
4

.Responder IP Initiator IP Count


Overview
Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Context Explorer
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom
Add Page
Add Graph
Add Summary Page
Add Table View
Editing Workflow
Name
ACP rule hit counters
Description
Table
Connection Events
Save
Cancel
Custom ▸ Custom Workflows
Page 1
Page Name
Rule Hits
Sort Type
Descending
Column 1
Column 2
Column 3
Column 4
Column 5
Sort Priority
Field
Access Control
Count
Initiator IP
Responder IP

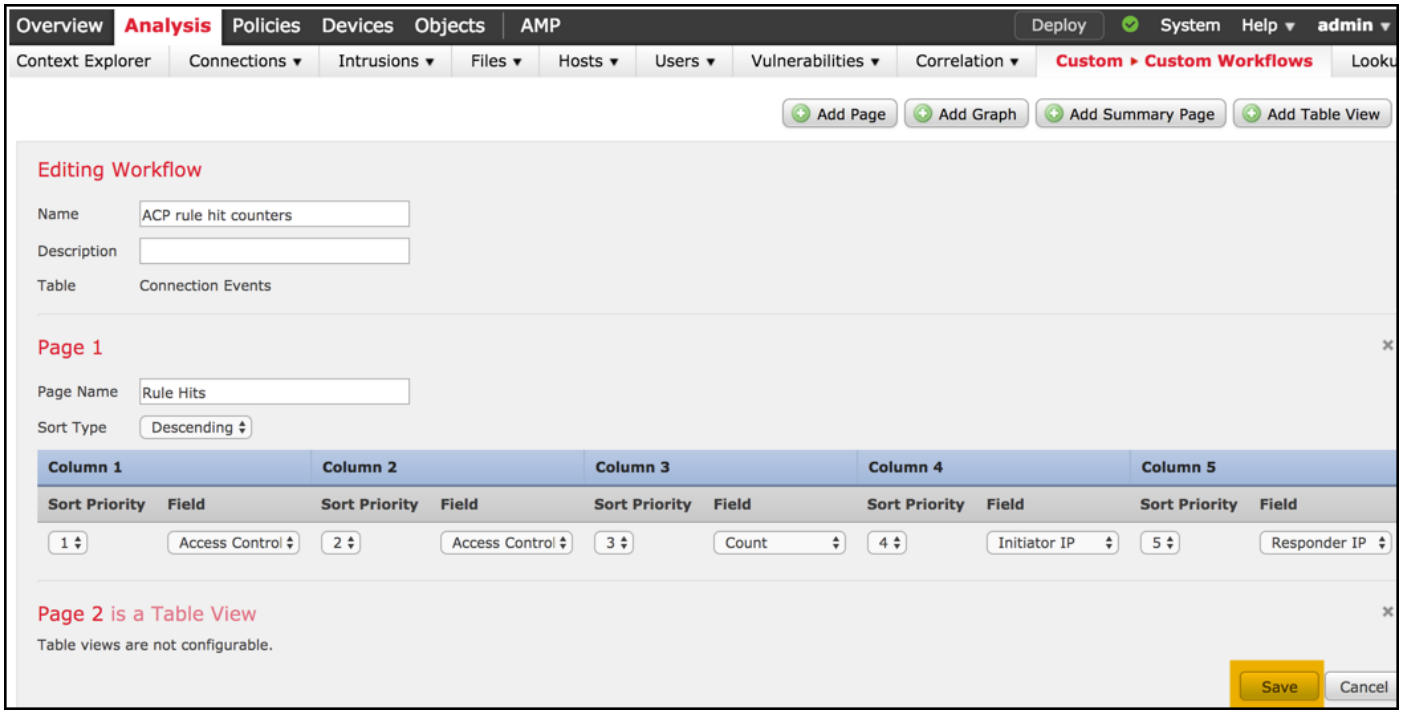
الخطوة 5

.


Analysis
Policies
Devices
Objects
AMP
Deploy
System
Help
admin
Connections
Intrusions
Files
Hosts
Users
Vulnerabilities
Correlation
Custom ▸ Custom Workflows
Add Page
Add Graph
Add Summary Page
Add Table View

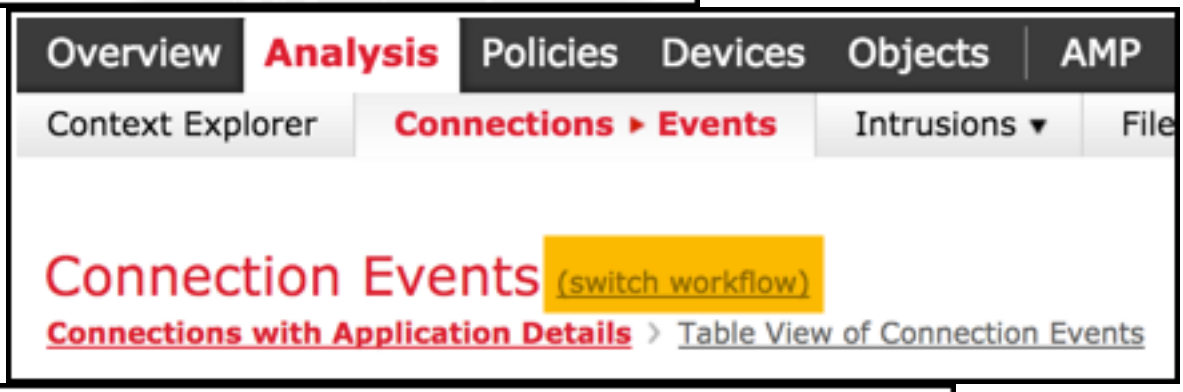
6

.

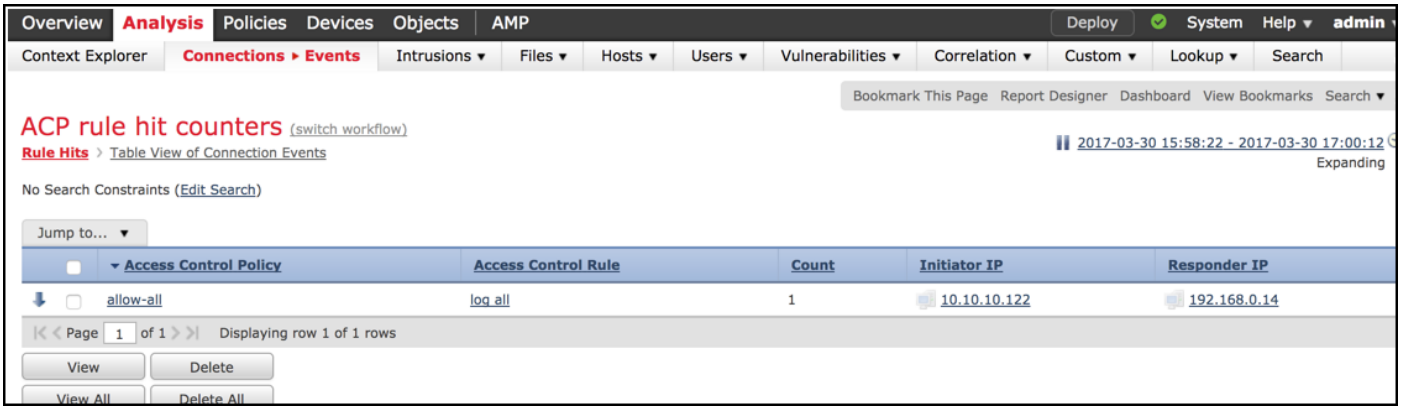


7

. **ACP** **< () Analysis**



. AC ACP



التحقق من الصحة

يمكن تحقيق طريقة لتأكيد عدادات الوصول إلى قاعدة التحكم على أساس القاعدة لجميع حركة المرور (بشكل عام) من الأمر CLISH **show access-control-config** (واجهة سطر الأوامر (CLI Shell)، وهو ما يتم توضيحه أدناه:

```
> show access-control-config

====================[ allow-all ]====================
                                  : Description
                          Default Action : Allow
        Default Policy : Balanced Security and Connectivity
                          Logging Configuration
                                 DC : Disabled
                          Beginning : Disabled
                                End : Disabled
                            Rule Hits : 0
                     Variable Set : Default-Set
                          (output omitted)…

------------------[ Rule: log all ]-----------------
                                Action : Allow
    Intrusion Policy : Balanced Security and Connectivity
                                : ISE Metadata

                      Source Networks : 10.10.10.0/24
                 Destination Networks : 192.168.0.0/24
                                        URLs
                          Logging Configuration
                                 DC : Enabled
                          Beginning : Enabled
                                End : Enabled
                              Files : Disabled
                            Rule Hits : 3
                     Variable Set : Default-Set

                          (output omitted) …
```

استكشاف الأخطاء وإصلاحها

باستخدام الأمر **firewall-engine-debug** يمكنك تأكيد ما إذا كان يتم تقييم تدفق حركة المرور مقابل قاعدة التحكم في الوصول المناسبة:

```
> system support firewall-engine-debug
```

```
Please specify an IP protocol: icmp
Please specify a client IP address: 10.10.10.122
Please specify a server IP address: 192.168.0.14
Monitoring firewall engine debug messages

AS 2 I 0 New session 1 192.168.0.14-0 < 10.10.10.122-8
AS 2 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 1 192.168.0.14-0 < 10.10.10.122-8
-> 0, vlan 0, sgt tag: untagged, svc 3501, payload 0, client 2000003501, misc 0, user 9999997, icmpType 8, icmpCode
0
AS 2 I 0 no match rule order 1, id 2017150 dst network and GEO 1 192.168.0.14-0 < 10.10.10.122-8
AS 2 I 0 match rule order 3, 'log all', action Allow 1 192.168.0.14-0 < 10.10.10.122-8
AS 2 I 0 allow action 1 192.168.0.14-0 < 10.10.10.122-8
```

. FMC (GUI) . IP CLI . GUI (CLI) ACP

معلومات ذات صلة

- مهام سير العمل المخصصة
- بدء الاستخدام مع سياسات التحكم في الوصول
- 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).