Centro de administración de la potencia de fuego: Contadores de aciertos de la directiva del control de acceso de la visualización

Contenido

Introducción

Prerrequisitos

Este documento describe las instrucciones de crear los **flujos de trabajo de encargo** en un centro de administración de la potencia de fuego (FMC) que permita que el sistema visualice a los contadores de aciertos de la directiva del control de acceso (ACP) sobre la base global y de la por-regla. Esto es útil de resolver problemas si el flujo de tráfico hace juego la regla correcta. Es también útil conseguir la información sobre el uso general de las reglas del control de acceso, por ejemplo el control de acceso gobierna sin los golpes durante un largo período del tiempo pudo ser una indicación que la regla no está necesitada más y se podría quitar potencialmente con seguridad del sistema.

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

- Centro de administración virtual de la potencia de fuego (FMC) - versión de software 6.1.0.1 (estructura 53)
- Defensa de la amenaza de la potencia de fuego (FTD) 4150 - versión de software 6.1.0.1 (estructura 53)

> Nota: La información descrita en este documento es no corresponde al administrador de dispositivo de la potencia de fuego (FDM).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Productos Relacionados

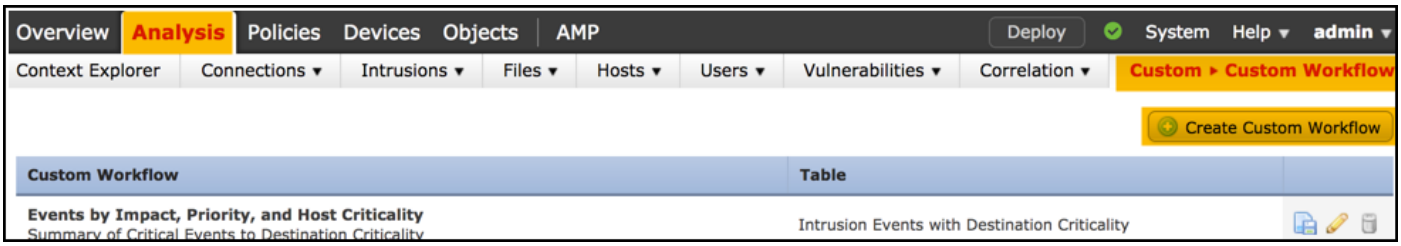
Este documento se puede también utilizar con estas versiones de software y hardware:

- Centro de administración de la potencia de fuego (FMC) - versión de software 6.0.x y más arriba
- Dispositivos manejados potencia de fuego - versión de software 6.1.x y más arriba

Configurar

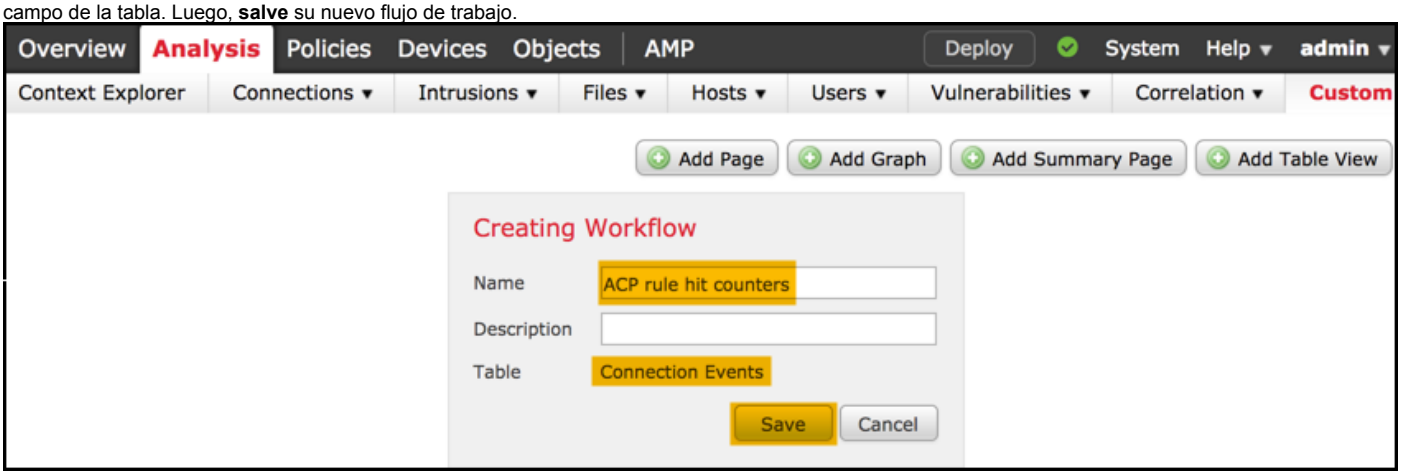
Paso 1

Para crear un flujo de trabajo de encargo, navegue al **análisis > a la aduana > los flujos de trabajo de encargo > crean el flujo de trabajo de encargo:**



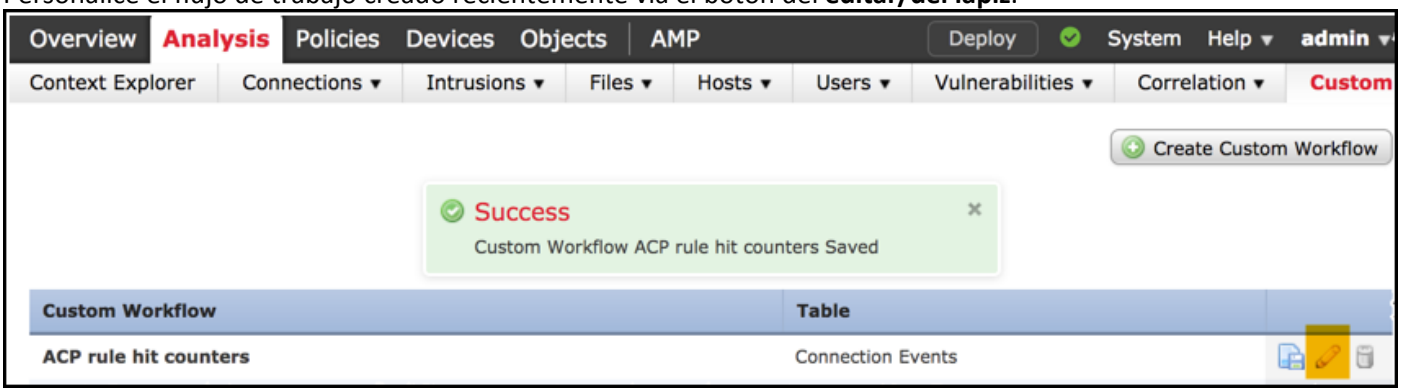
Paso 2

Defina el nombre **de encargo del flujo de trabajo**, por ejemplo los **contadores de aciertos de la regla ACP** y seleccione los **eventos de conexión** en un campo de la tabla. Luego, **salve** su nuevo flujo de trabajo.



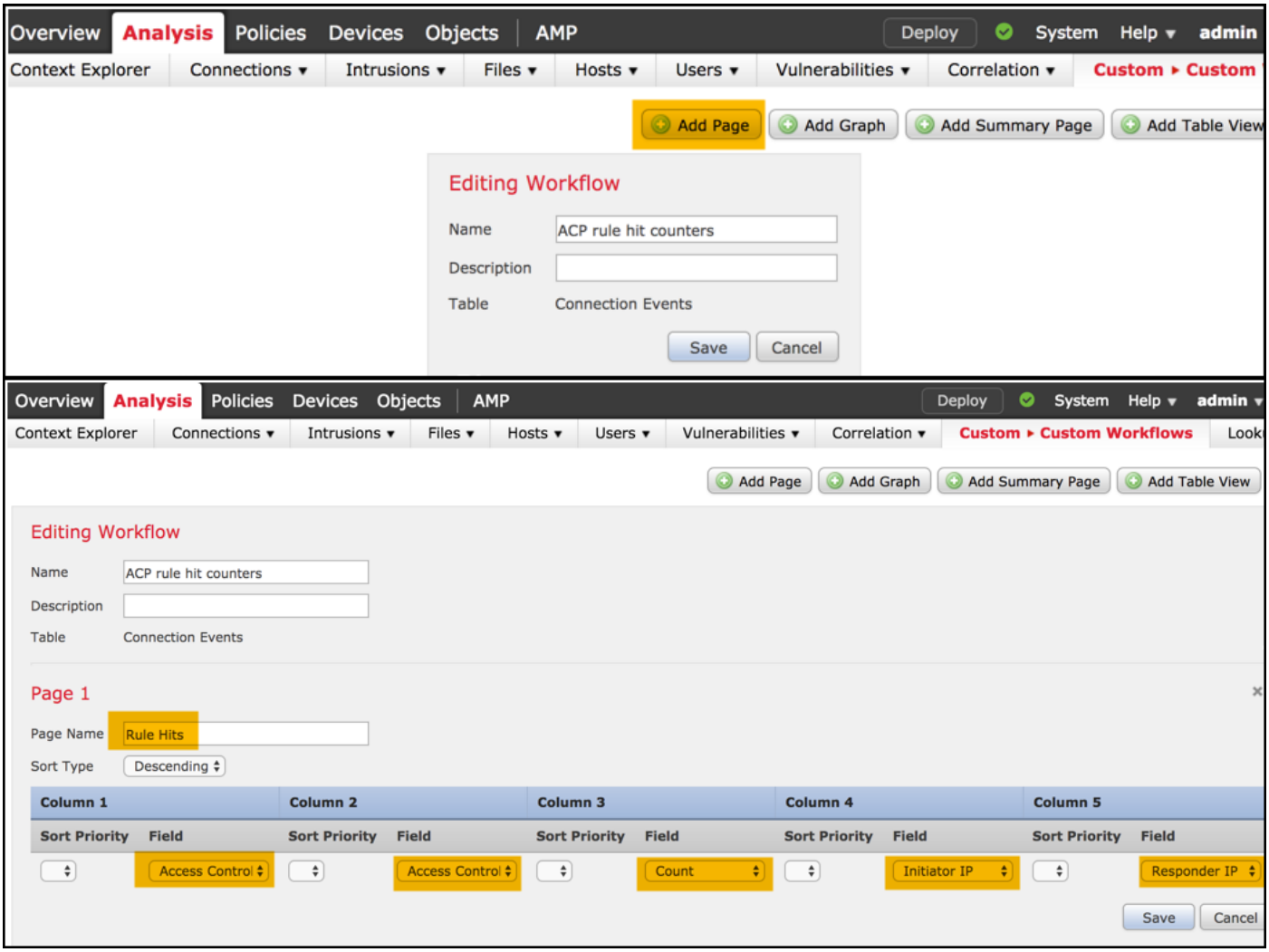
Paso 3

Personalice el flujo de trabajo creado recientemente vía el botón del **editar/del lápiz**.



Paso 4

Agregue una nueva página para un flujo de trabajo con la opción de **página del agregar**, defina su nombre y clasifique los campos de columna por la **directiva del control de acceso**, **regla del control de acceso** y por el **IP de la cuenta**, del **iniciador** y los campos **IP del respondedor**.

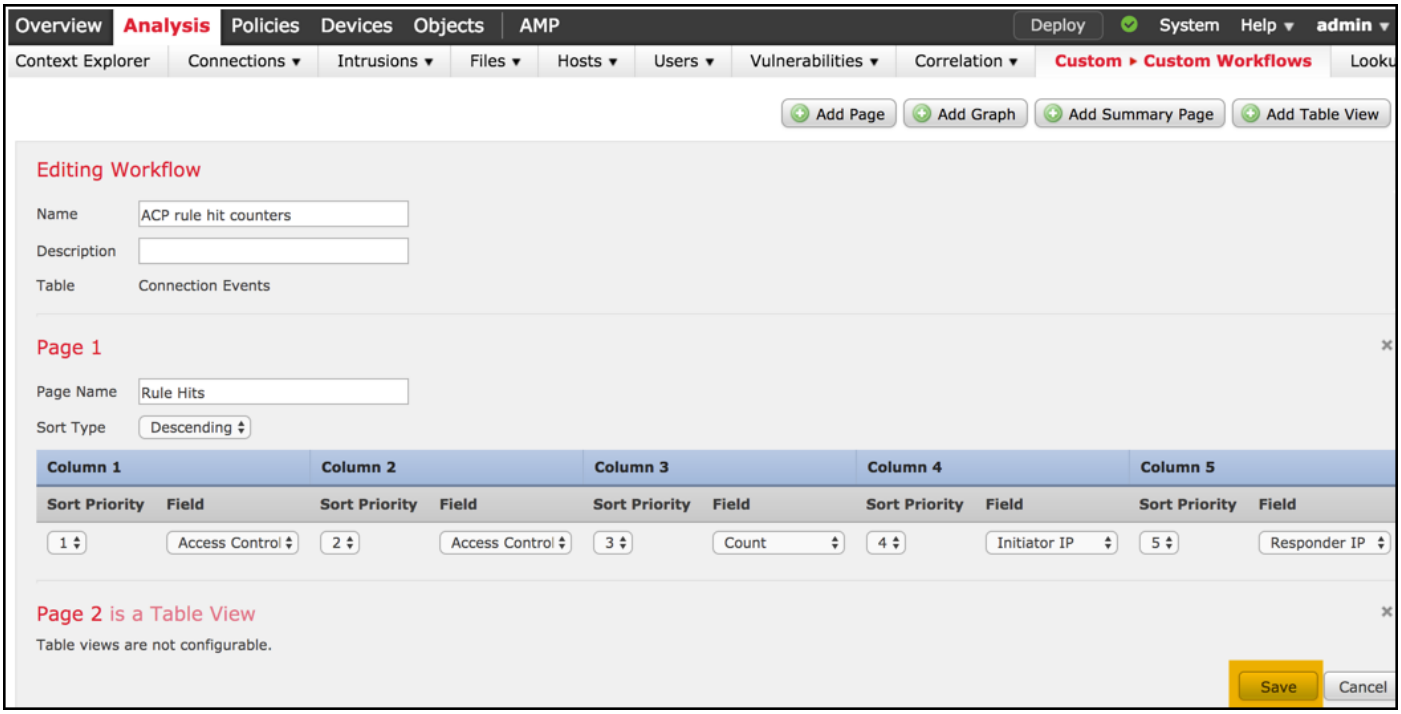


Paso 5

Agregue una segunda página con la opción de la **opinión de la tabla del agregar**.

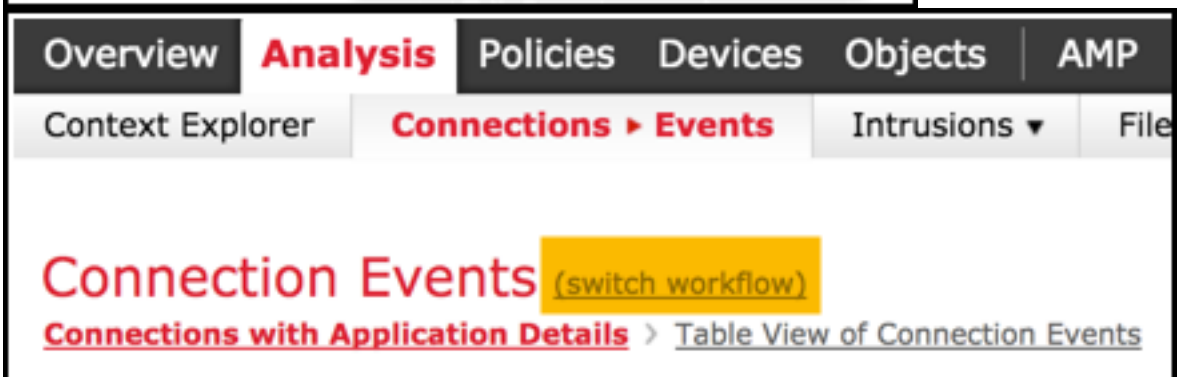
Paso 6

La opinión de la tabla no es configurable, por lo tanto apenas procede **a salvar** su flujo de trabajo.

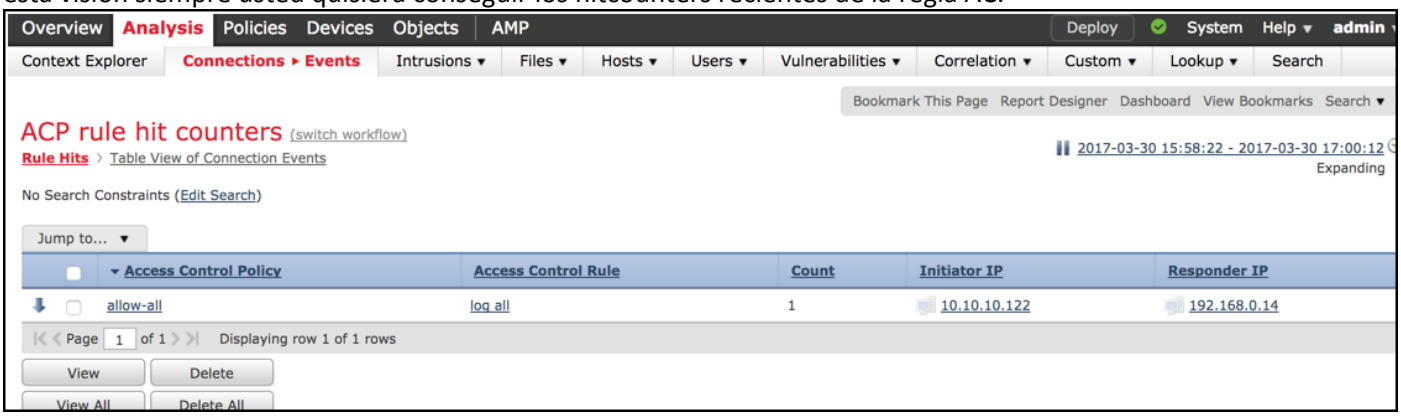


Paso 7

Navegue a los **eventos del análisis > de las conexiones** y al **flujo de trabajo del** switch de selección, después elija el flujo de trabajo creado recientemente nombrado los **contadores de aciertos de la regla ACP** y espere hasta que las recargas de la página.



La página se carga una vez, los contadores de aciertos de la regla por cada regla ACP se visualiza, apenas restaura esta visión siempre usted quisiera conseguir los hitcounters recientes de la regla AC.



Verificación

Una manera de confirmar a los contadores de aciertos de la regla del control de acceso sobre la base de la regla para todo el tráfico (global) se puede alcanzar del comando de los acceso-control-**config de la demostración** FTD CLISH (SHELL CLI), que se demuestra abajo:

```
> 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)
```

Troubleshooting

Con el comando del Firewall-motor-**debug** usted puede confirmar si el flujo de tráfico está evaluado contra la regla apropiada del control de acceso:

```
> 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

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

Cuando usted compara a los contadores de aciertos para la regla ACP nombrada **registro todo** usted nota que la línea de comando (CLI) y las salidas GUI no hacen juego. La razón es que borran después de cada implementación de política del control de acceso y se aplican a los contadores de aciertos CLI a todo el tráfico global y no a los IP Addresses específicos. En la otra mano, FMC GUI mantienen los contadores la base de datos, así que pueden visualizar los datos históricos basados en un tiempo de trama seleccionado.

Información Relacionada

- Flujos de trabajo de encargo
- Introducción con las directivas del control de acceso
- Soporte Técnico y Documentación - Cisco Systems