

Centre de Gestion de puissance de feu : Compteurs de hit de stratégie de contrôle d'accès d'affichage

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Conditions préalables

Ce document décrit les instructions de créer des **processus faits sur commande à un** centre de Gestion de puissance de feu (FMC) qui permet au système pour afficher des compteurs de hit de la stratégie de contrôle d'accès (ACP) sur la base globale et de par-règle. Il est utile dépanner ce si la circulation apparie la règle correcte. Il est également utile d'obtenir des informations sur l'utilisation générale des règles de contrôle d'accès, par exemple le contrôle d'accès ordonne sans des hit pendant une période étendue du temps pourrait être une indication que la règle n'est plus nécessaire et pourrait être potentiellement sans risque retiré du système.

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

- Centre virtuel de Gestion de puissance de feu (FMC) - version de logiciel 6.1.0.1 (construction 53)
- Défense contre des menaces de puissance de feu (FTD) 4150 - version de logiciel 6.1.0.1 (construction 53)

Remarque: Les informations décrites dans ce document s'appliquent pas applicable au gestionnaire de périphériques de puissance de feu (FDM).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Produits connexes

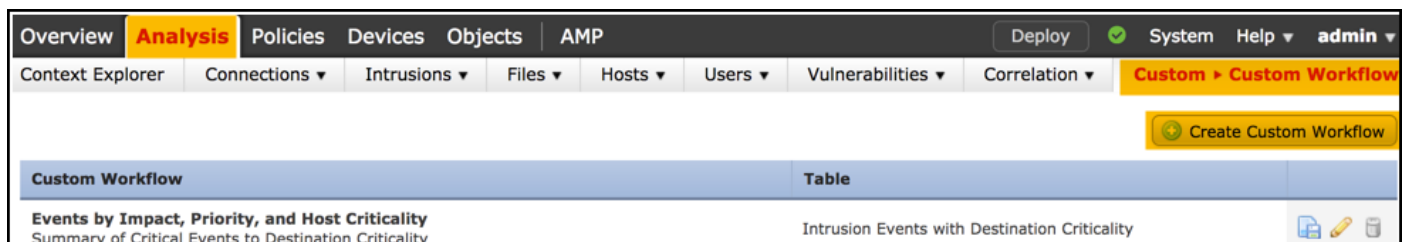
Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Centre de Gestion de puissance de feu (FMC) - version de logiciel 6.0.x et plus élevé
- La puissance de feu a géré des appliances - la version de logiciel 6.1.x et plus élevé

Configurez

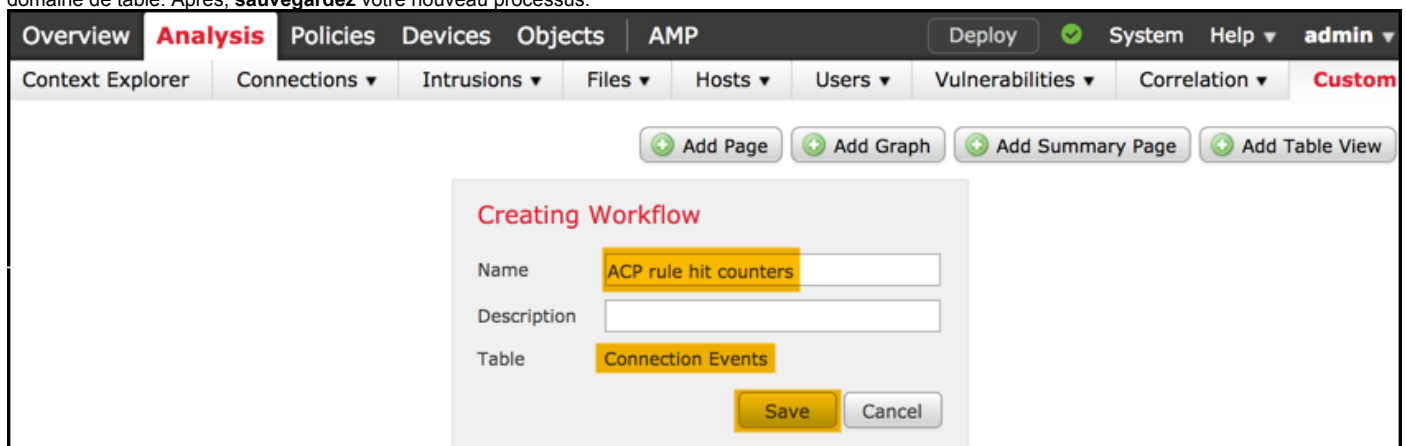
Étape 1

Afin de créer un processus fait sur commande, naviguez vers **l'analyse > la coutume > des processus faits sur commande > crée le processus fait sur commande** :



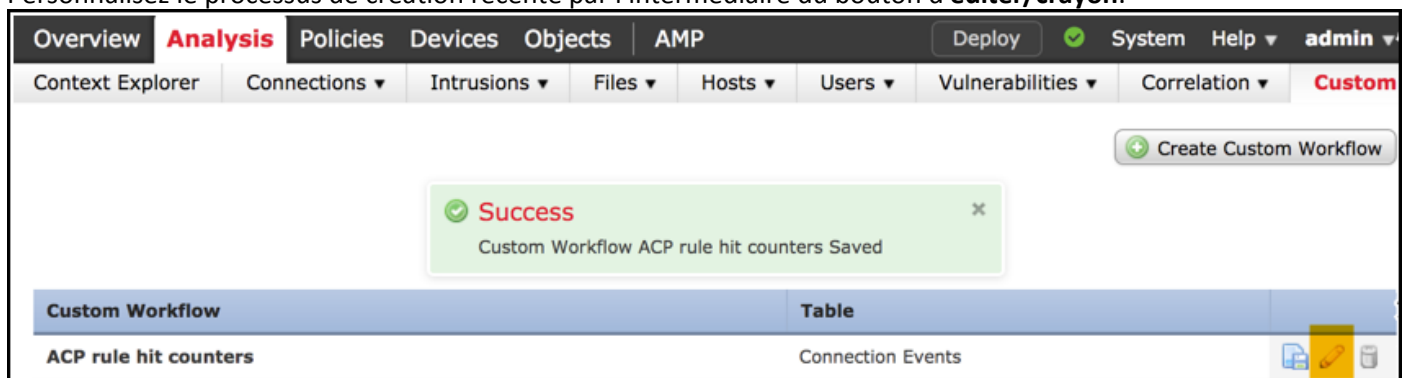
Étape 2

Définissez le nom **fait sur commande de processus**, par exemple des **compteurs de hit de règle ACP** et des **événements** choisis de **connexion** dans un domaine de table. Après, **savegardez** votre nouveau processus.



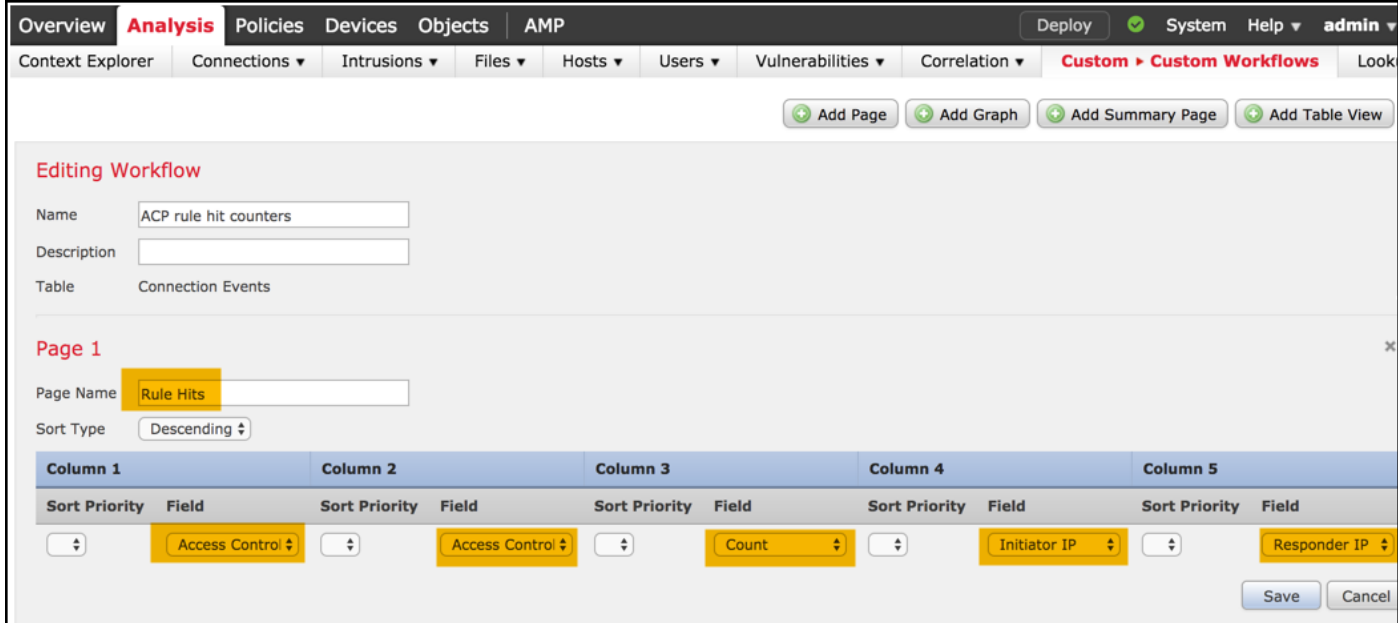
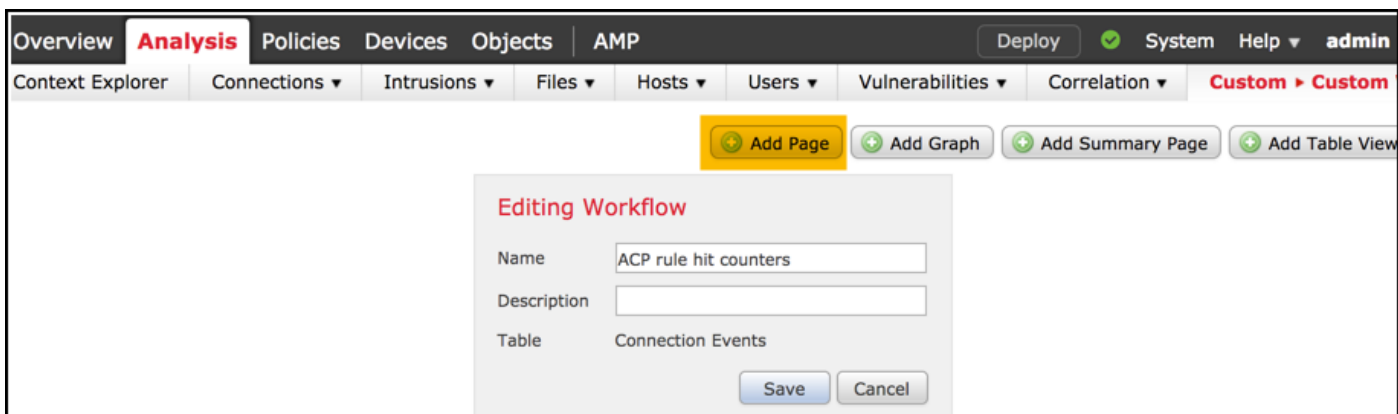
Étape 3

Personnalisez le processus de création récente par l'intermédiaire du bouton d'**éditer/crayon**.



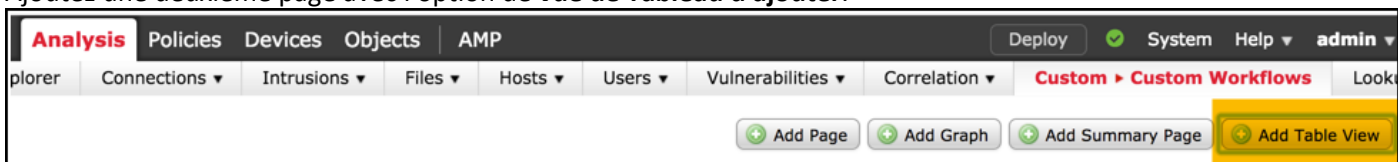
Étape 4

Ajoutez une nouvelle page pour un processus avec l'option de **page d'ajouter**, définissez son nom et triez les champs de colonne par **stratégie de contrôle d'accès**, **règle de contrôle d'accès** et des champs par l'**IP de compte**, de **demandeur** et de **responder IP**.



Étape 5

Ajoutez une deuxième page avec l'option de **vue de Tableau d'ajouter**.



Étape 6

La **vue de Tableau** n'est pas configurable, par conséquent poursuit juste **pour sauvegarder** votre processus.

Overview **Analysis** Policies Devices Objects AMP Deploy System Help admin

Context Explorer Connections Intrusions Files Hosts Users Vulnerabilities Correlation **Custom** Custom Workflows Looku

+ Add Page + Add Graph + Add Summary Page + Add Table View

Editing Workflow

Name:
 Description:
 Table: Connection Events

Page 1

Page Name:
 Sort Type: Descending

Column 1	Column 2	Column 3	Column 4	Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
1	Access Control	2	Access Control	3	Count
4	Initiator IP	5	Responder IP		

Page 2 is a Table View
 Table views are not configurable.

Save Cancel

Étape 7

Naviguez vers des **événements d'analyse > de connexions** et le **processus de commutateur** choisi, puis choisissez le processus de création récente nommé des **compteurs de hit de règle ACP** et attendez jusqu'à ce que les recharges de page.

Overview **Analysis** Policies Devices Obj

Context Explorer Connections Intrusions

Events
Security Intelligence Events

Overview **Analysis** Policies Devices Objects AMP

Context Explorer **Connections** Events Intrusions File

Connection Events (switch workflow)

Connections with Application Details > [Table View of Connection Events](#)

Overview **Analysis** Policies Devices Objects AMP

Context Explorer **Connections** Events Intrusions File

Connection Events ×

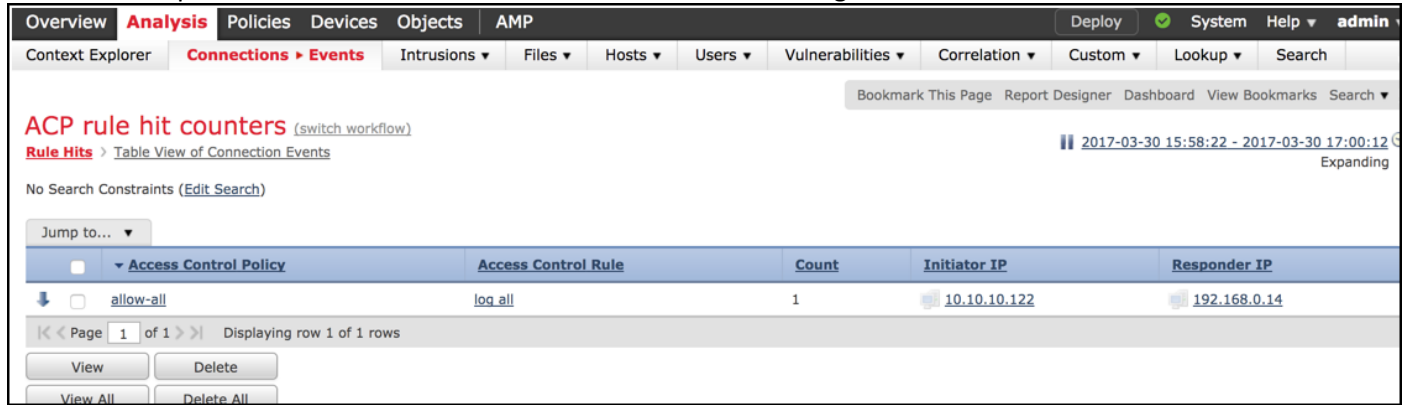
ACP rule hit counters

Connection Events

Connections by Application

Connections with Application Details > [Table View of Connection Events](#)

Une fois que la page est chargée, les compteurs de hit de règle par chaque règle ACP sont affichés, régénèrent juste cette vue lorsque vous voudriez obtenir des hitcounters récents de règle à C.A.



The screenshot shows the Cisco ISE GUI interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Analysis' tab is active, and the 'Connections > Events' sub-tab is selected. The main content area displays 'ACP rule hit counters' with a table view of connection events. The table has columns for 'Access Control Policy', 'Access Control Rule', 'Count', 'Initiator IP', and 'Responder IP'. One row is visible for the 'allow-all' policy and 'log all' rule, with a count of 1, initiator IP 10.10.10.122, and responder IP 192.168.0.14. The page also shows search constraints, a 'Jump to...' dropdown, and pagination controls.

Vérifiez

Une manière de confirmer des compteurs de hit de règle de contrôle d'accès sur la base de règle pour tout le trafic (globalement) peut être réalisée de la commande d'Access-contrôle-**config d'exposition** FTD CLISH (SHELL CLI), qui est expliquée ci-dessous :

```
> 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)
```

Dépannez

Avec la commande de Pare-feu-engine-**debug** vous pouvez confirmer si la circulation est évaluée contre la règle appropriée de contrôle d'accès :

```
> 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
```

Quand vous comparez les compteurs de hit pour la règle ACP nommée **se connectent tous que** vous notez que la ligne de commande (CLI) et les sorties GUI ne s'assortissent pas. La raison est que les compteurs de hit CLI sont effacés après chaque déploiement de stratégie de contrôle d'accès et s'appliquent à tout le trafic globalement et pas à l'les adresses IP spécifiques. Sur l'autre main, le GUI FMC maintiennent les compteurs dans la base de données, ainsi il peut afficher les données historiques basées sur une période sélectionnée.

[Informations connexes](#)

- [Processus faits sur commande](#)
- [Obtenir commencé par des stratégies de contrôle d'accès](#)
- [Support et documentation techniques - Cisco Systems](#)