

Firepower Management Center : アクセスコントロール ポリシー ヒット カウンタの表示

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

前提条件

ACP Firepower Management CenterFMC

要件

このドキュメントに特有の要件はありません。

- Firepower Management CenterFMC- 6.1.0.1 53
- Firepower Threat DefenseFTD4150 - 6.1.0.1 53

注：このドキュメントで説明する情報は、Firepower Device Manager (FDM) には当てはまりません。

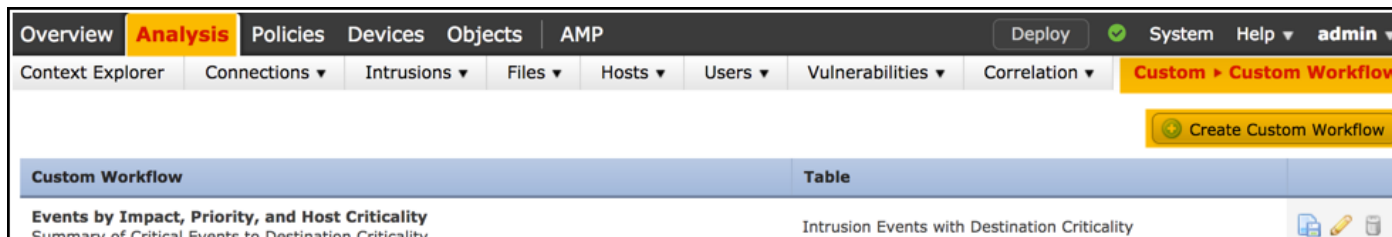
このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Firepower Management CenterFMC- 6.0.x
- Firepower - 6.1.x

設定

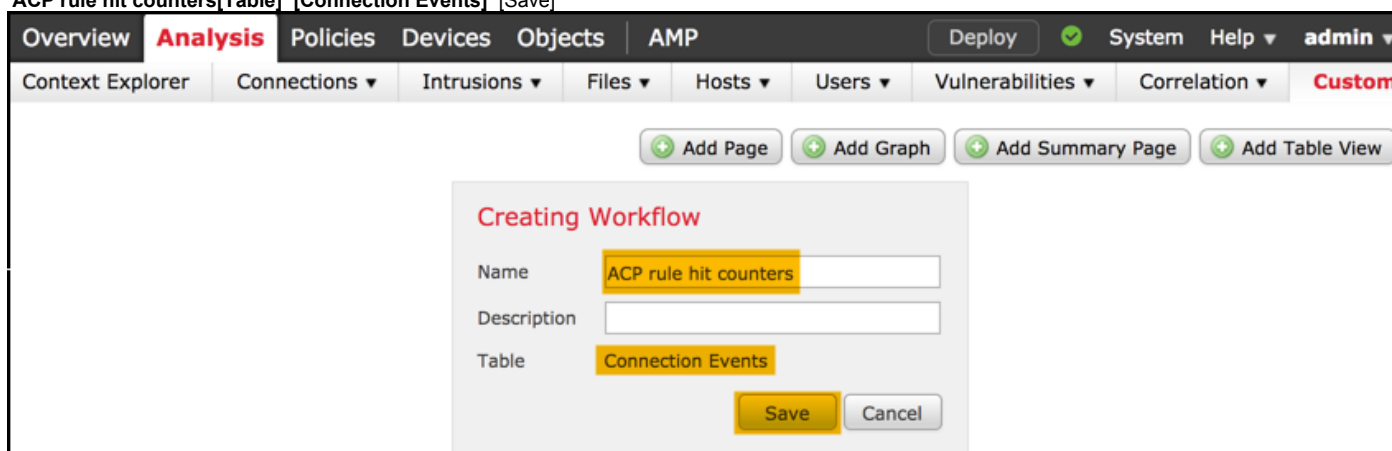
1

カスタム ワークフローを作成するには、[分析 (Analysis)] > [カスタム (Custom)] > [カスタム ワークフロー (Custom Workflows)] > [カスタムワークフローの作成 (Create Custom Workflow)] の順に移動します。

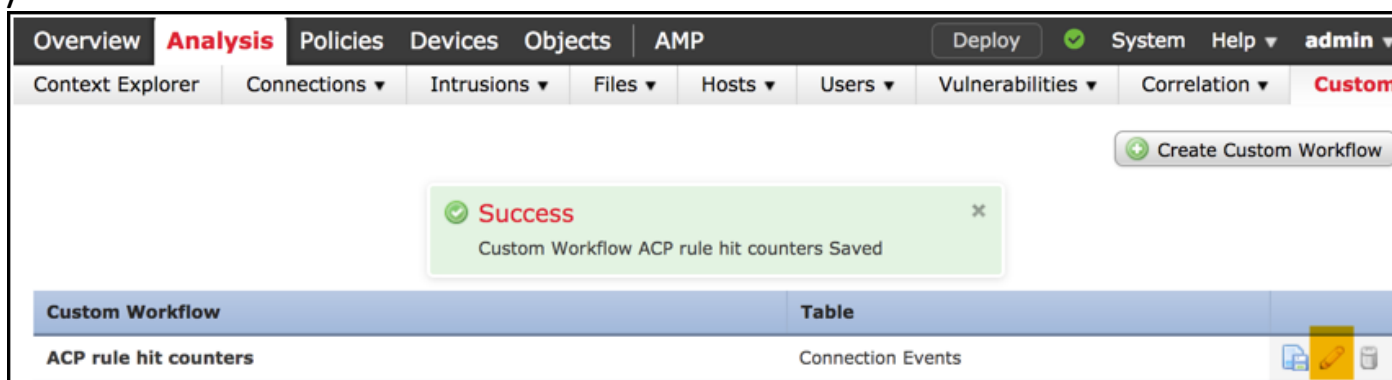


2

ACP rule hit counters[Table] [Connection Events] [Save]

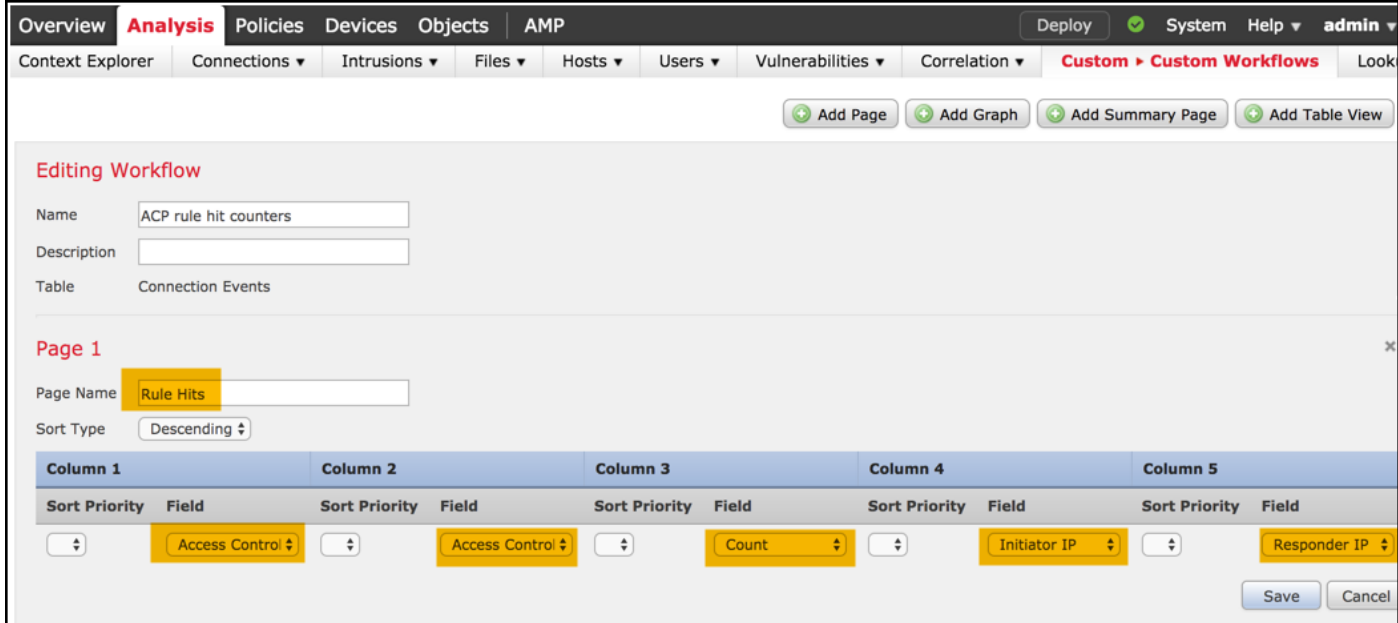
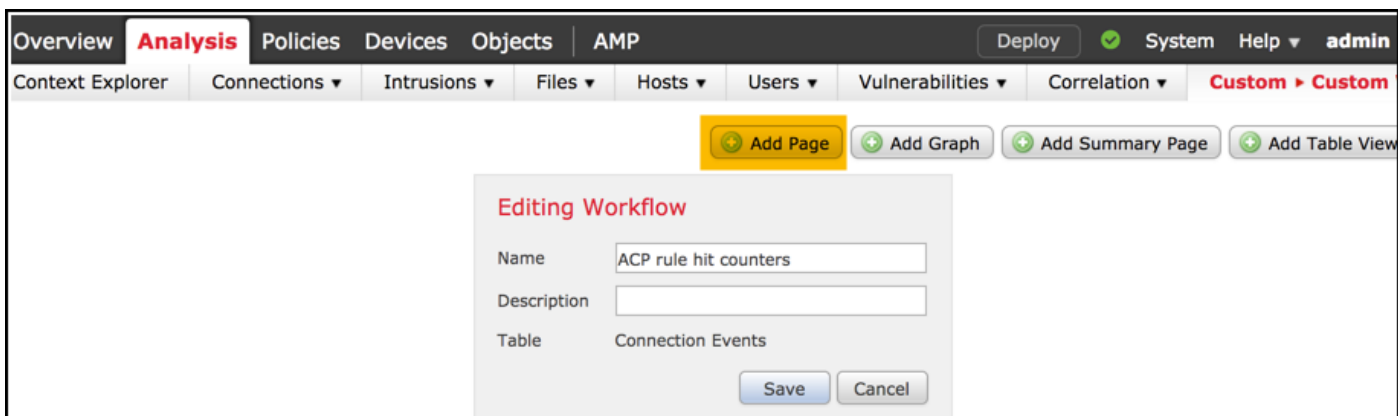


3



4

[Add Page] [Access Control Policy] [Access Control Rule] [Count][IPInitiator IP][IPResponder IP]



手順 5

[Add Table View] 2



6

[Table View] [Save]

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:

Column 1	Column 2	Column 3	Column 4	Column 5	
Sort Priority	Field	Sort Priority	Field	Sort Priority	Field
<input type="text" value="1"/>	<input type="text" value="Access Control"/>	<input type="text" value="2"/>	<input type="text" value="Access Control"/>	<input type="text" value="3"/>	<input type="text" value="Count"/>
<input type="text" value="4"/>	<input type="text" value="Initiator IP"/>	<input type="text" value="5"/>	<input type="text" value="Responder IP"/>		

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

Save Cancel

7

[Analysis] > [Connections] > [Events] [switch workflow] [ACPACP rule hit counters]

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

[s](#) > [Table View of Connection Events](#)

Access Control Policy	Access Control Rule	Count	Initiator IP	Responder IP
allow-all	log all	1	10.10.10.122	192.168.0.14

確認

全トラフィックのアクセスコントロールルールヒットカウンタをルールベースで(グローバルに)確認するには、FTD CLISH (CLI SHELL) の **show access-control-config** コマンドを使用します。その例を以下に示します。

```
> 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)
```

トラブルシューティング

firewall-engine-debug コマンドを使用すると、トラフィックフローが適切なアクセスコントロールルールに照らし合わせて評価されているかどうかを確認することができます。

> **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

log all ACP CLI GUI CLI IP FMC GUI

関連情報

- [カスタム ワークフロー](#)
- [アクセス コントロール ポリシー入門](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)