

アクセスルールごとのヒットカウントを表示するためのFiresight Management Centerの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、カスタムワークフロー/イベントビューアページを設定して、アクセスルール名ごとの接続ヒットカウントを示す方法について説明します。設定は、ヒットカウントに関連付けられたルール名フィールドの基本的な例と、必要に応じて追加フィールドを追加する方法を示します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER の知識
- Firesight Management Center内の基本的なナビゲーションに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Centerバージョン6.1.X以降
- マネージド脅威防御/火力センサーに適用可能

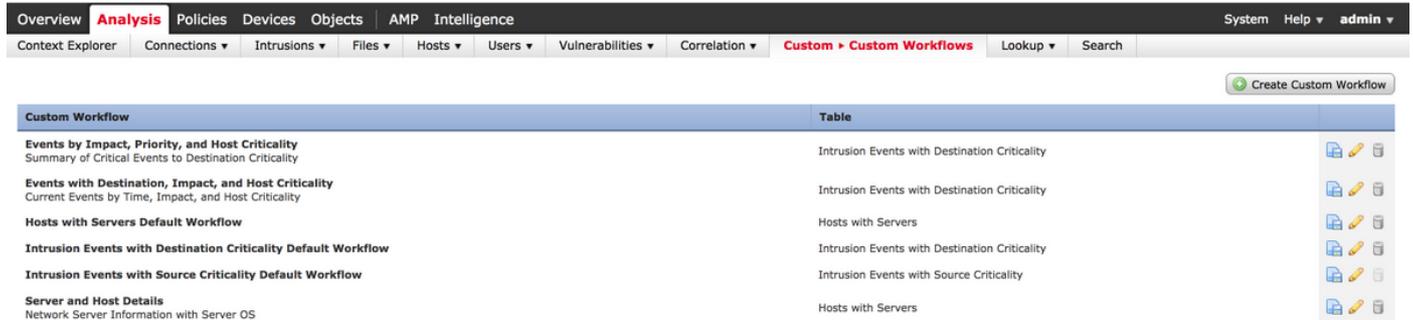
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

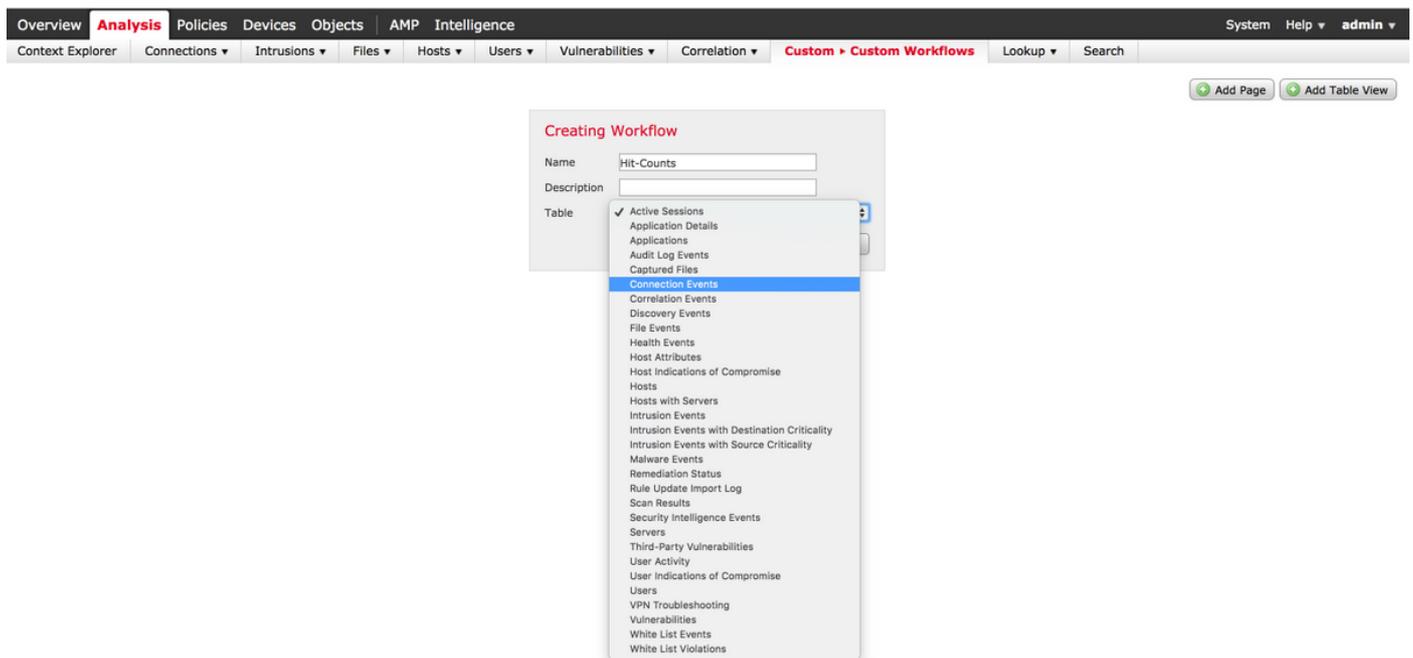
設定

ステップ1：管理者権限でFiresight Management Centerにログインします。

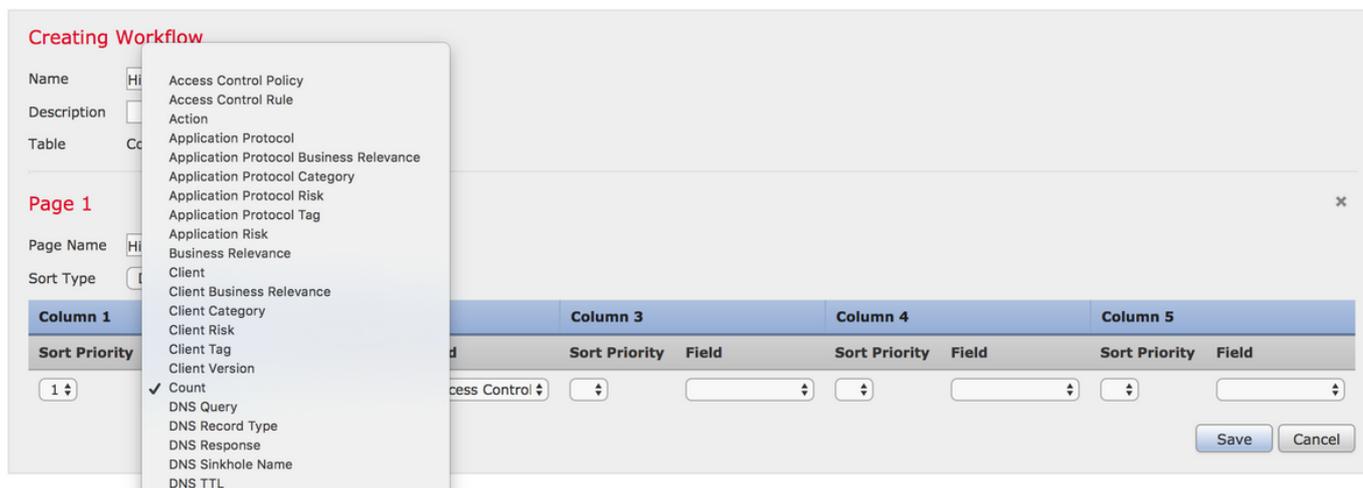
ログインが正常に完了したら、図に示すように、[Analysis] > [Custom] > [Custom Workflows]に移動します。



ステップ2:[Create Custom Workflow]をクリックし、図に示すようにパラメータを選択します。



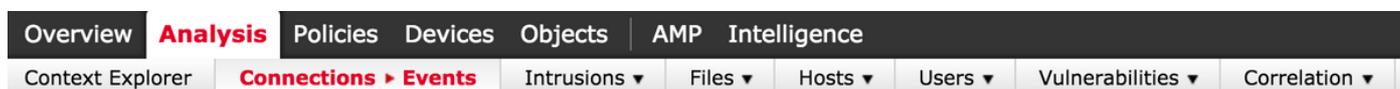
ステップ3:[Connection Events]というテーブルフィールドを選択し、ワークフロー名を入力して、[Save]をクリックします。ワークフローを保存したら、次の図に示すように[Add Page]をクリックします。



注：最初の列は[カウント(Count)]にする必要があり、追加の[列(Column)]では、ドロップダウンから使用可能なフィールドから選択できます。この場合、最初の列はカウントで、2番目の列はアクセスコントロールルールです。

ステップ4：ワークフローページが追加されたら、[保存(Save)]をクリックします。

ヒットカウントを表示するには、図に示すように、[Analysis] > [Connections] > [Events]に移動し、[Switch Workflows]をクリックします。



Connection Events ×

Connections > Table View of Connection Events

- Connection Events
- Connections by Application
- Connections by Initiator
- Connections by Port
- Connections by Responder
- Connections over Time
- Hit-Counts**
- Traffic by Application
- Traffic by Initiator
- Traffic by Port
- Traffic by Responder
- Traffic over Time •
- Unique Initiators by Responder
- Unique Responders by Initiator

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		
↓	Allow		10.1.1.5		10.76.77.50		
↓	Allow		10.1.1.5		10.76.77.50		
↓	Allow		10.1.1.5		172.217.7.238	USA	

ステップ5：図に示すように、ドロップダウンから、作成したカスタムワークフロー（この場合はヒットカウント）を選択します。

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

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

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

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。