

Настройте центр управления Firesight для отображения количеств соответствия на правило доступа

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ описывает, как настроить пользовательскую страницу потока операций/просмотра событий для изображения количества соответствия соединения на имя правила доступа. Конфигурация показывает базовый пример поля имени правила, привязанного к количеству соответствия и как добавить дополнительные поля при необходимости.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание технологии огневой мощи
- Навигация знания основ в Центре управления Firesight

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 6.1. X Центра управления огневой мощи и выше
- Применимый к управляемым Датчикам Защиты/Огневой мощи Угрозы

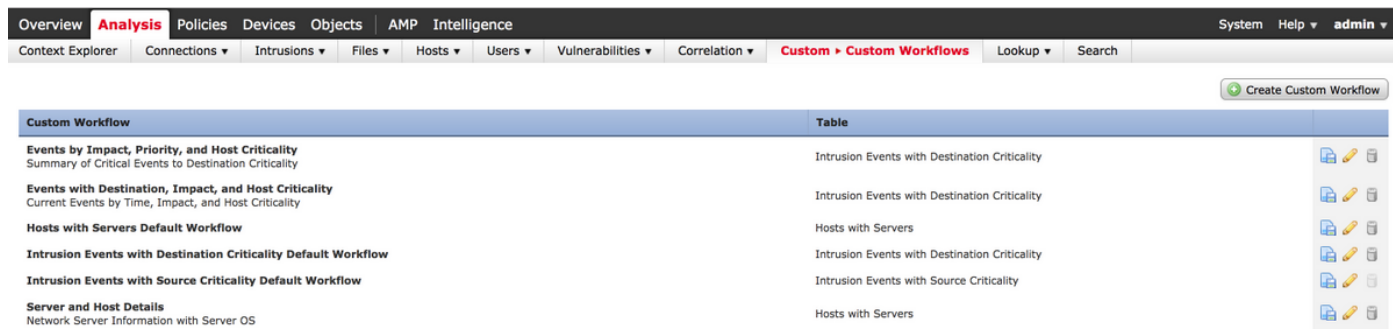
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

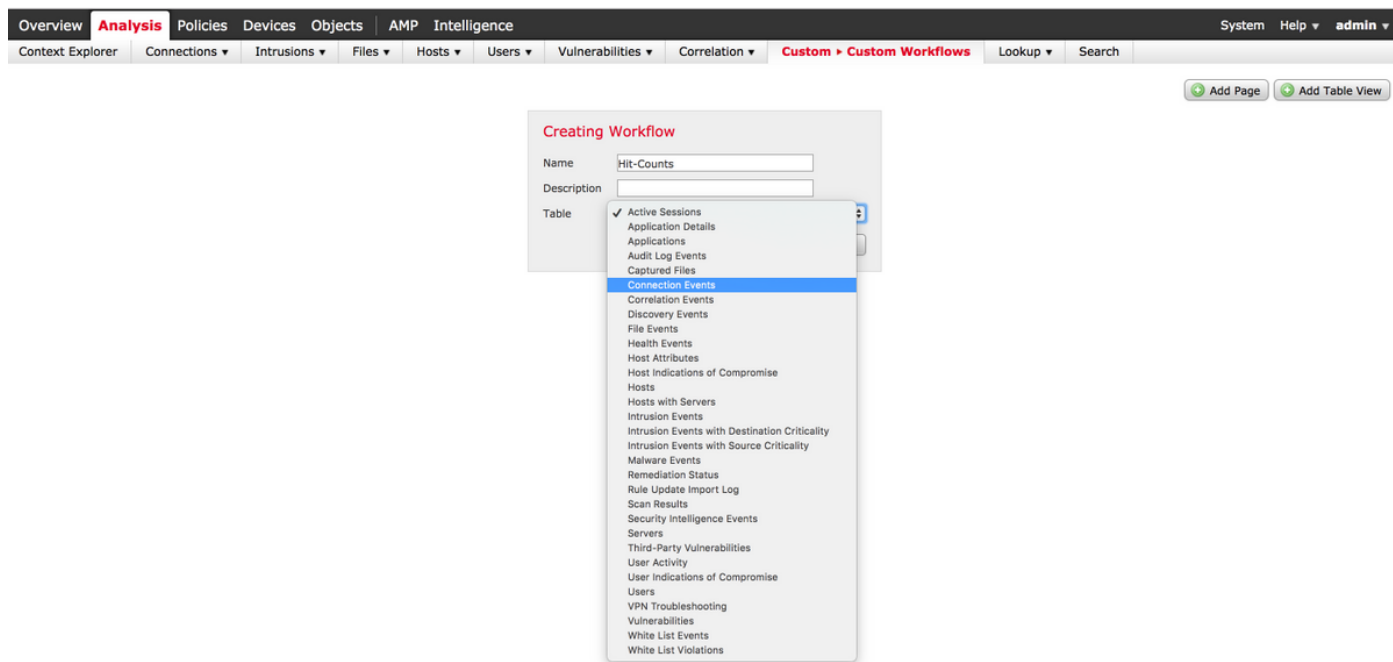
Конфигурации

Шаг 1. Вход в систему к Центру управления Firesight с администраторскими привилегиями.

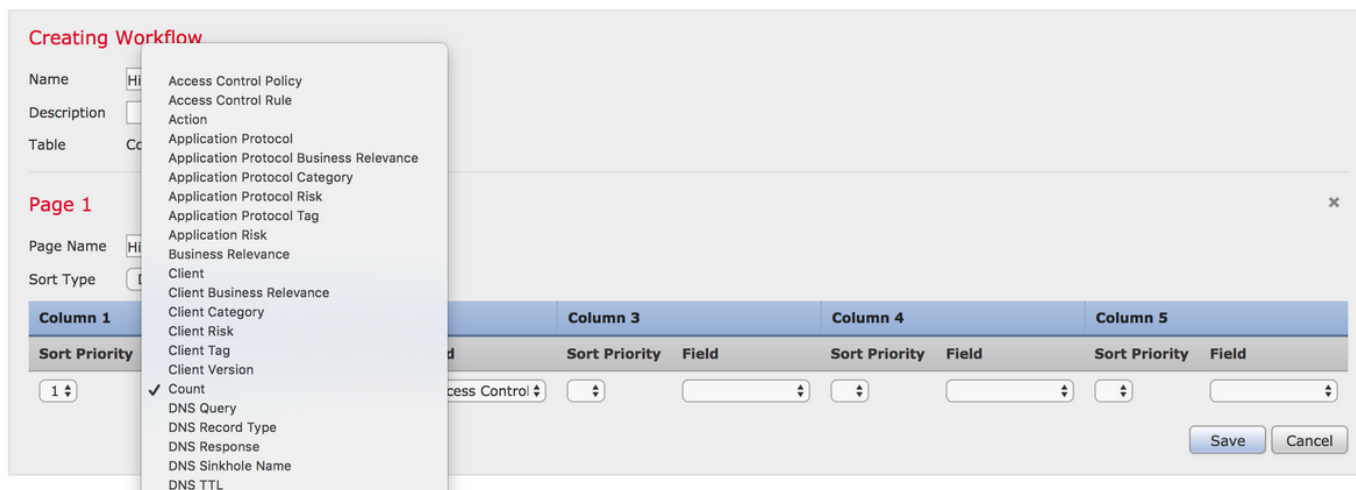
Как только вход в систему успешен, перешли к **Анализу > Пользовательский > Пользовательские Потоки операций**, как показано в образе:



Шаг 2. Щелкните по **Create Custom Workflow** и выберите параметры как показано в образе:



Шаг 3. Выберите поле таблицы как **События подключения** и введите имя Потока операций, затем щелкните по **Save**. Как только поток операций сохранен, щелкните по **Странице Add** как показано в образе:



Примечание: Первый столбец должен быть количеством, и затем в дополнительном Столбце можно выбрать среди доступных полей из выпадающего. В этом случае первый столбец является количеством, и второй столбец является Правилем Управления доступом.

Шаг 4. . Как только страница потока операций добавлена, щелкните по **Save**.

Для просмотра количества соответствия перейдите к **Анализу>> Events (sentence) Соединений** и щелкните по **Switch Workflows**, как показано в образе:

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer **Connections > Events** Intrusions Files Hosts Users Vulnerabilities Correlation

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

Table View of Connection Events

Last 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		
2017-07-19 08:47:13	Allow		10.1.1.5		10.76.77.50		
2017-07-19 08:47:08	Allow		10.1.1.5		10.76.77.50		
2017-07-19 08:47:08	Allow		10.1.1.5		172.217.7.238	USA	

Шаг 5. . От выпадающего выберите Custom Workflow, который вы создали (в этом случае

количества Соответствия), как показано в образе:

Hit-Counts (switch workflow)
Hit-Counts Based on Access Control

No Search Constraints (Edit Search)

2017-07-19 07:36:06 - 2017-07-19 08:52:39 Expanding

Count	Access Control Rule
66	Default-Allow

Jump to...
Displaying row 1 of 1 rows Page 1 of 1

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.