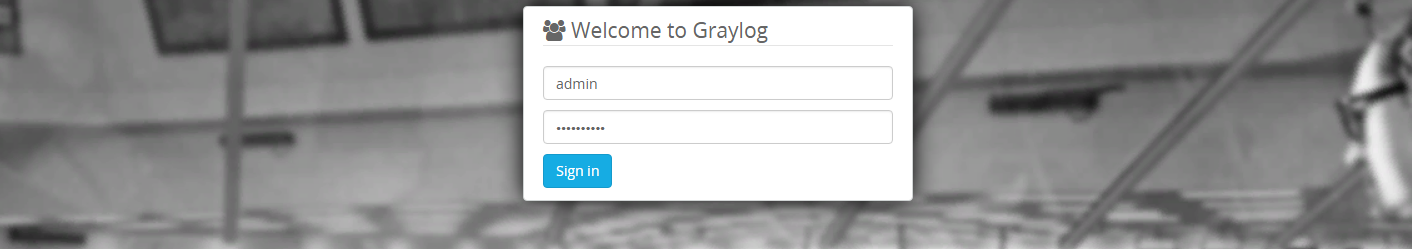
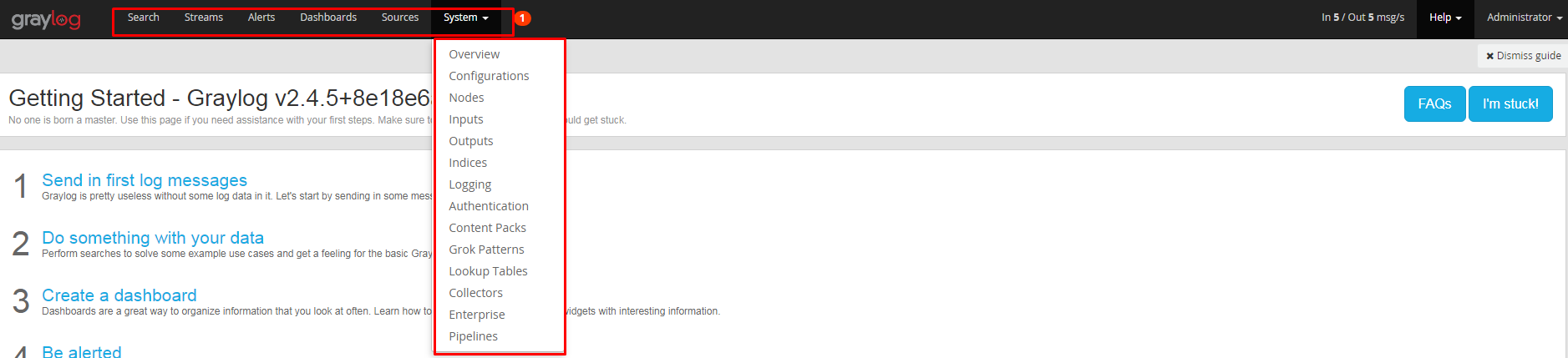
**Инструкция администратора**

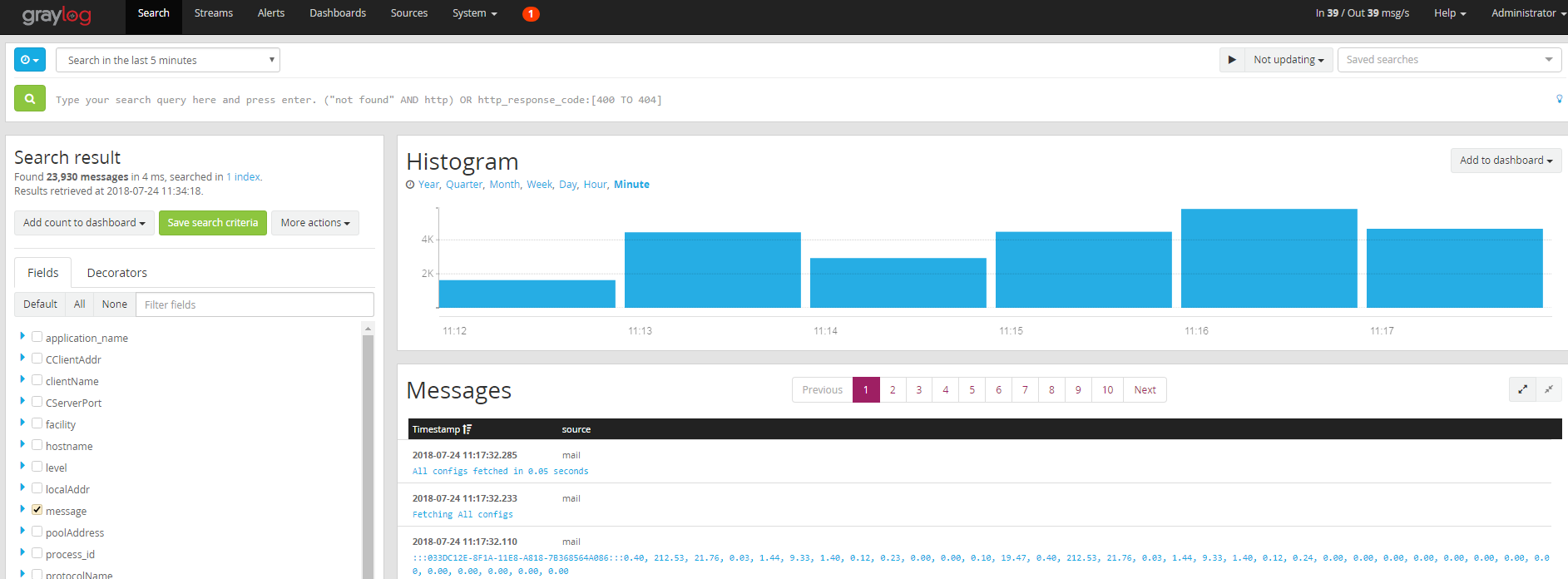
1. **Переходим по адресу** https://адрес\_сервера в панель администрирования



1. **В интерфейсе**, панель навигации



1. **Search** – поиск по всем событиям, используя все inputs и экстракторы. Поддерживает регулярные выражения.



Пример запросов:

Сообщения, содержащие ssh:

ssh

Сообщения, содержащие термин ssh или login:

ssh login

Сообщения, содержащие точную фразу авторизации SSH:

"ssh login

Сообщения, где в поле поле login:

type:ssh

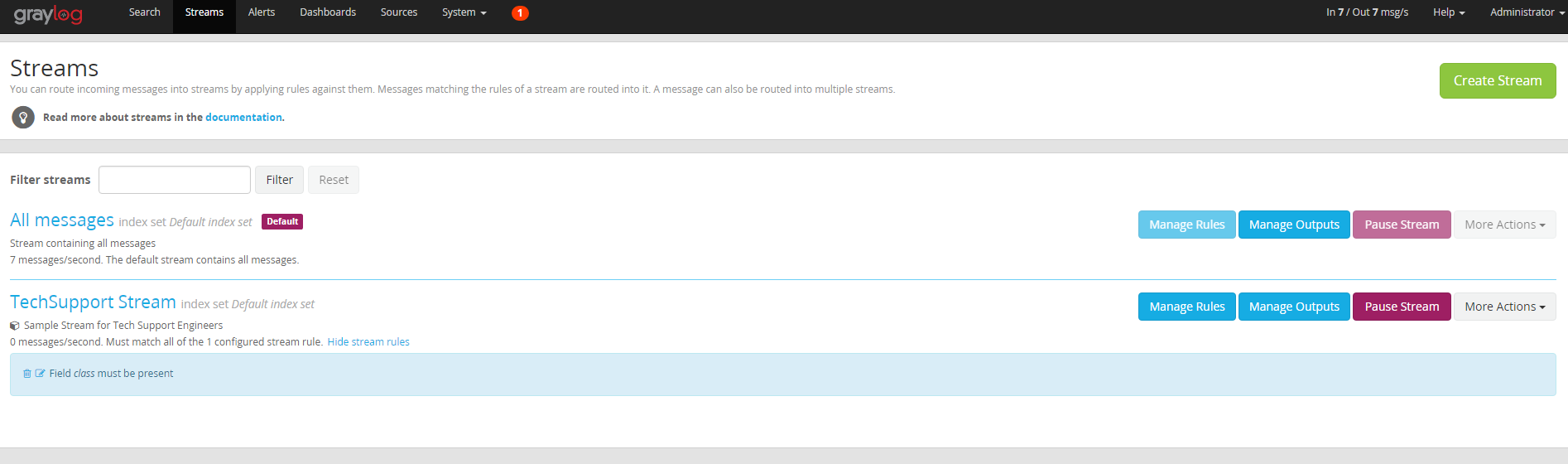
Сообщения, где поле включает ssh или login:

Тип:(ssh login)

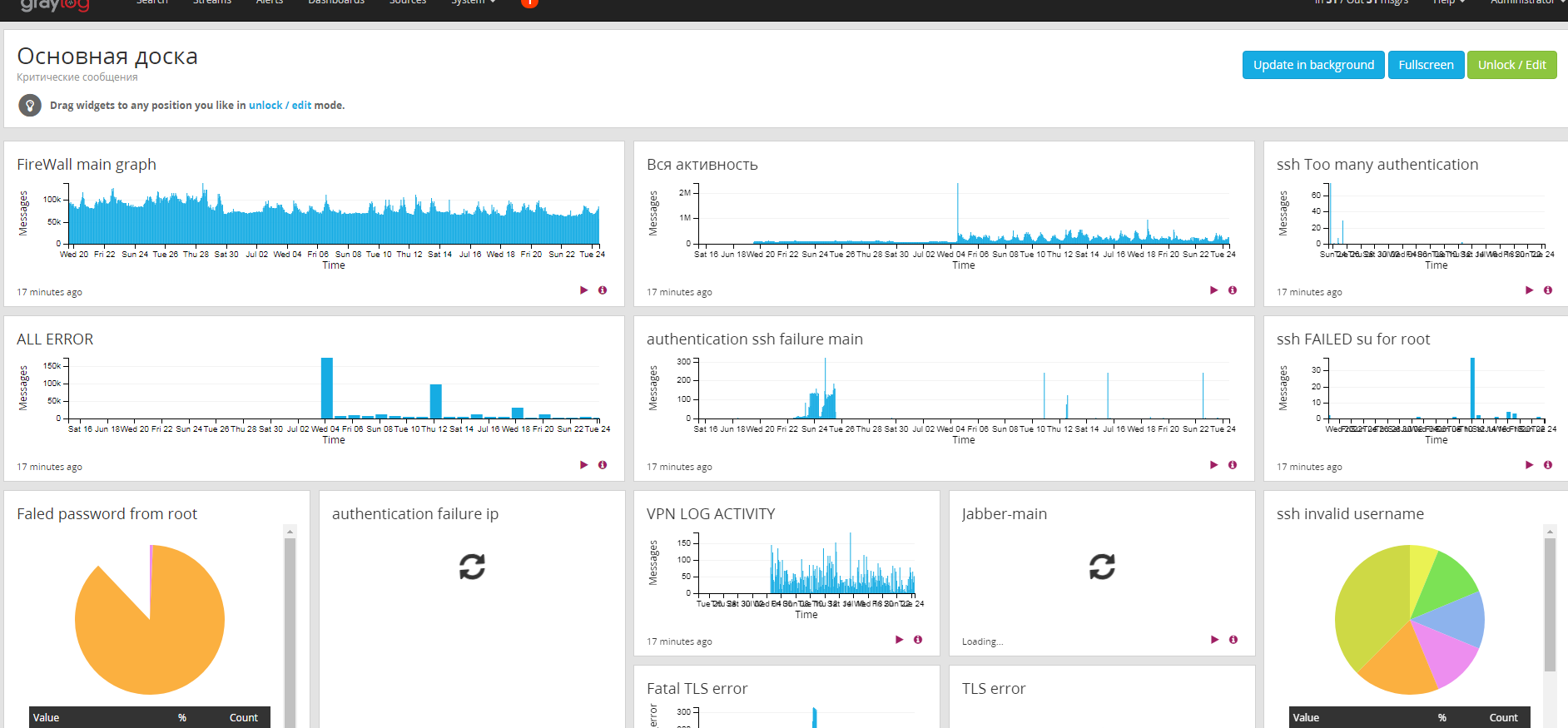
Сообщения, где в поле включает точную фразу SSH login:

Тип:"SSH login

1. **Steams** – возможность разделить потоки

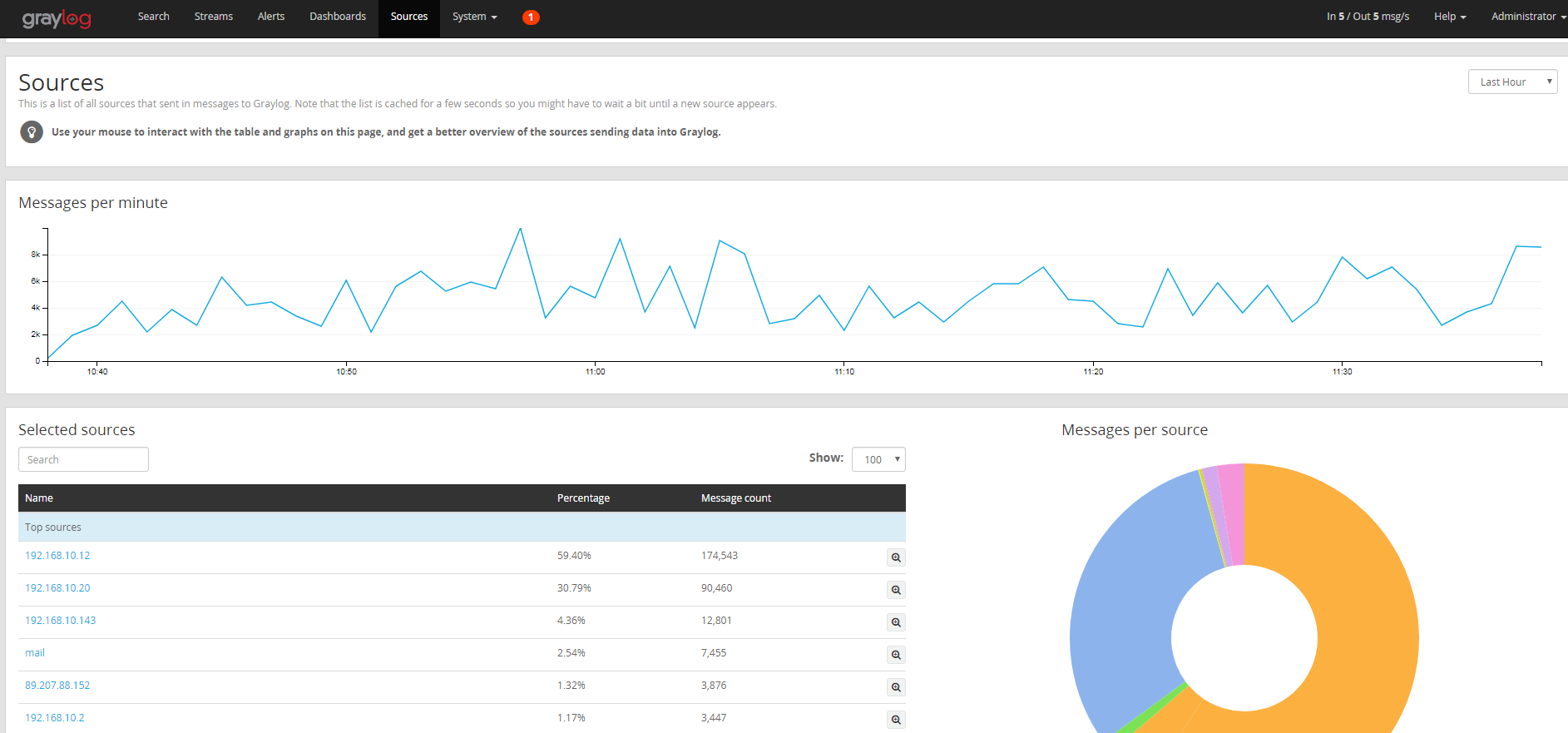


1. **Alerts** – уведомления, возможность при наступлении определенных событий слать уведомления.
2. **Dashboard** – вывод отсортированной информации ввиде : графиков, диаграмм, таблиц, виджетов и карт.

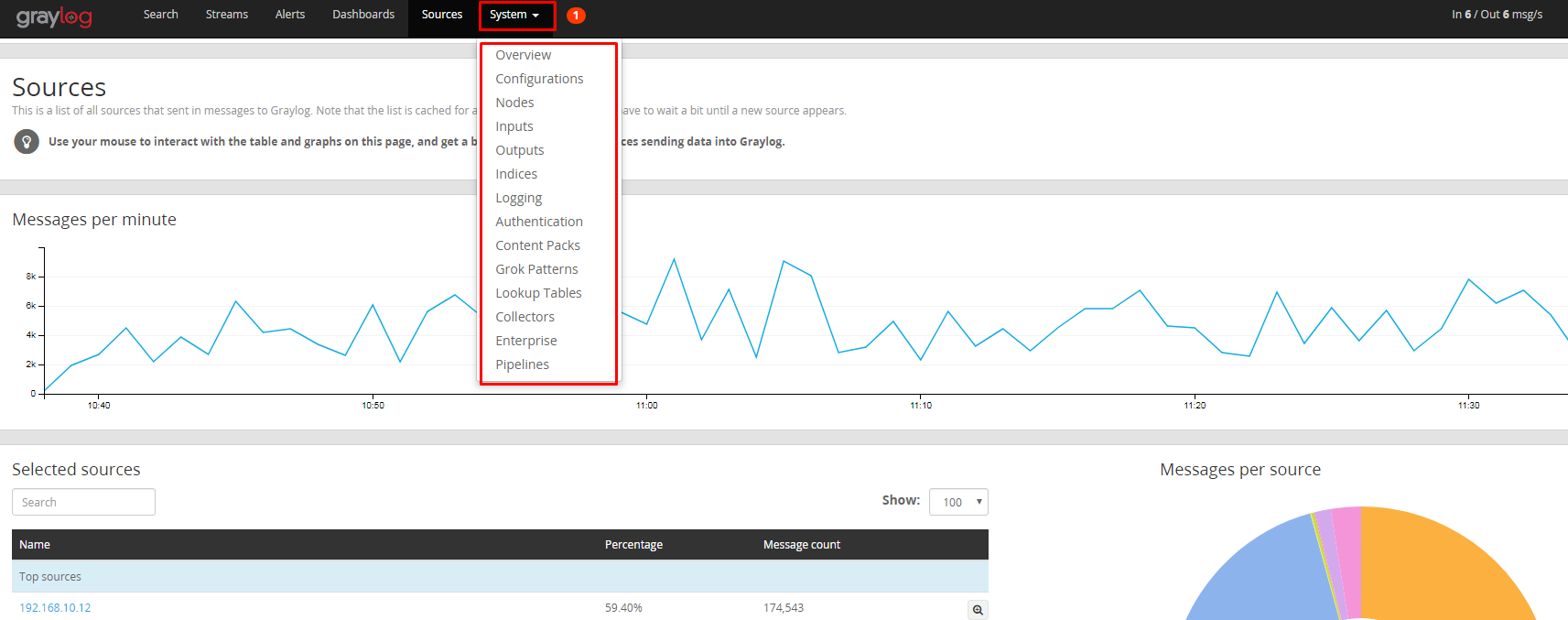


Возможность делать не ограниченное количество таких экранов информации по нужной тематике.

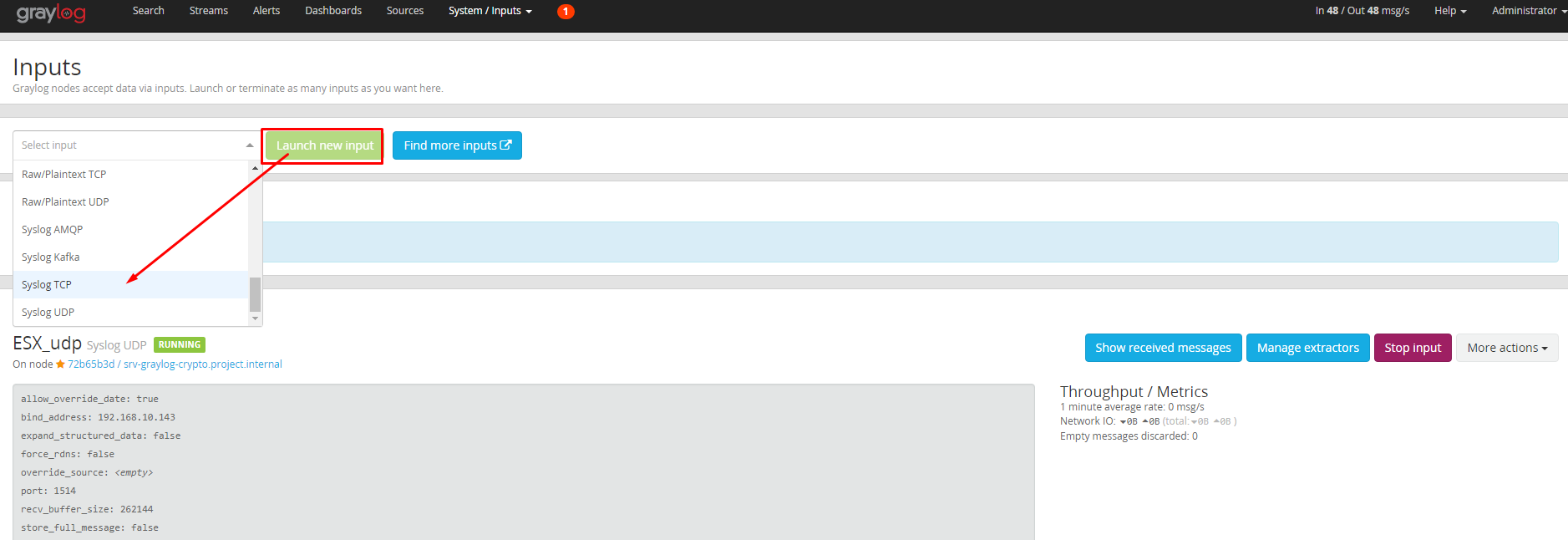
1. **Sources** – информация о хостах передающих логи



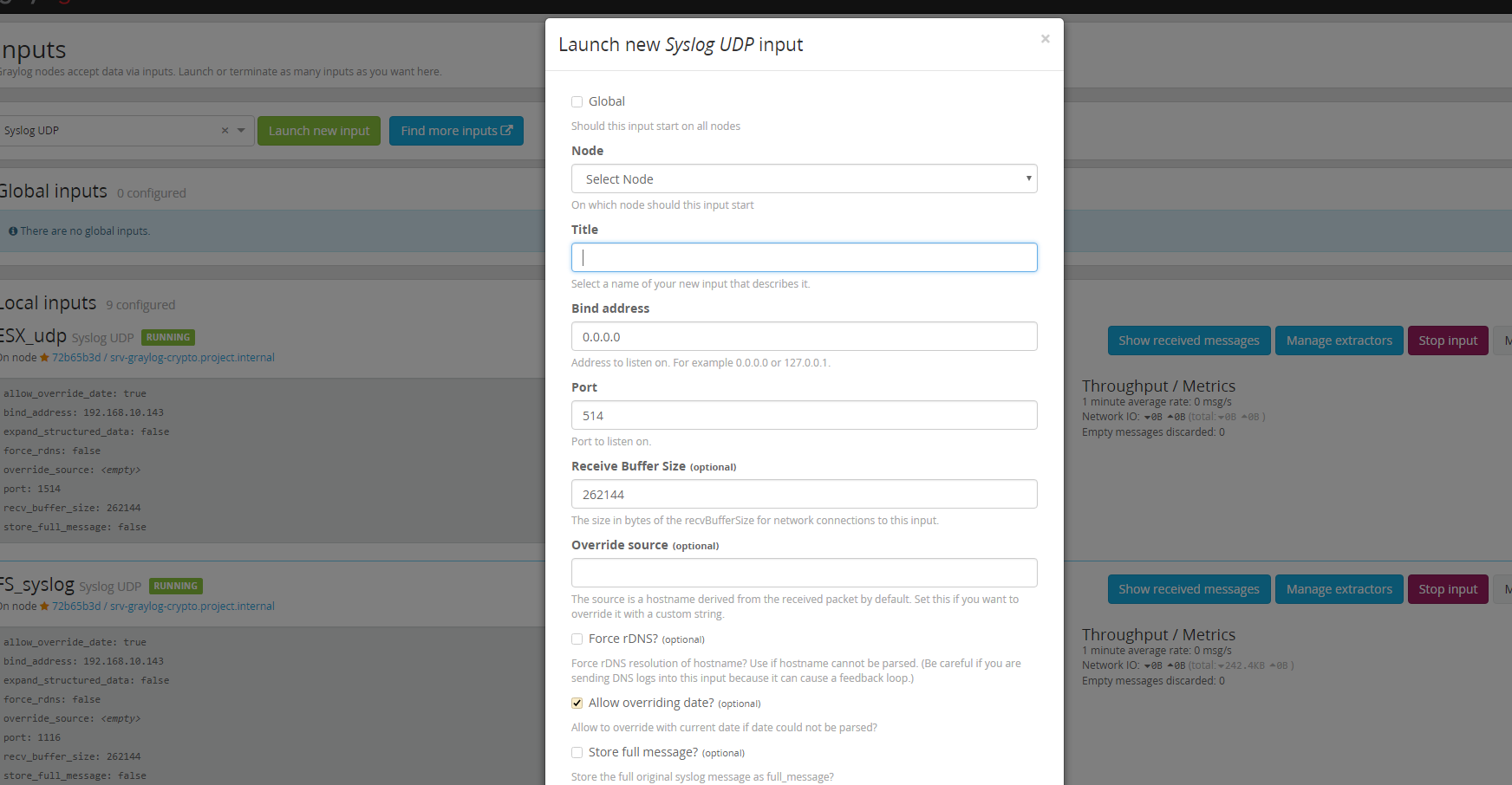
1. **System** – меню с системными настройками.



1. **Inputs** – добавление источников траффика

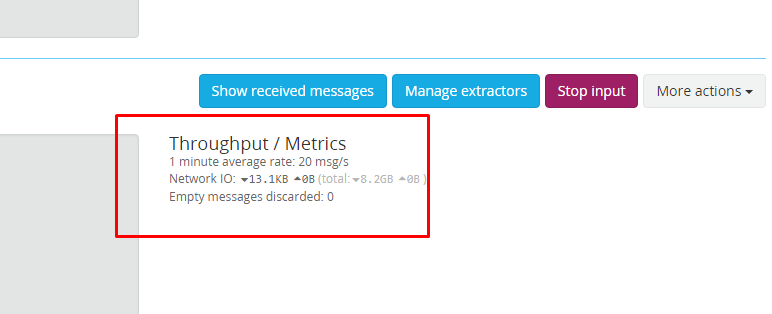


Выбираем нужный тип получения обычно это syslog.

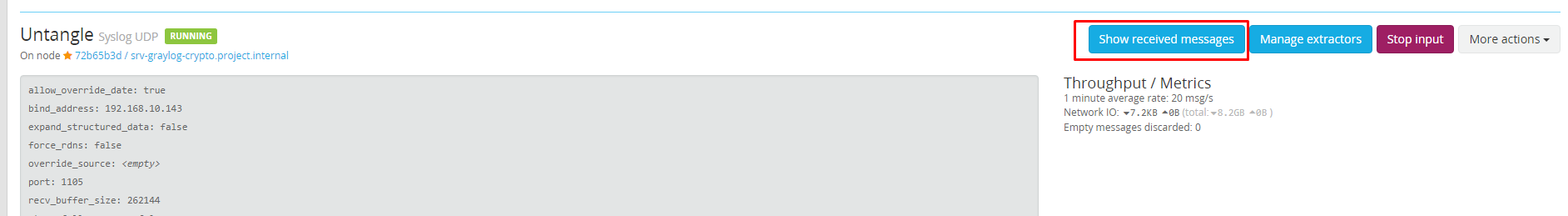


Вводим настройки, тут все просто.

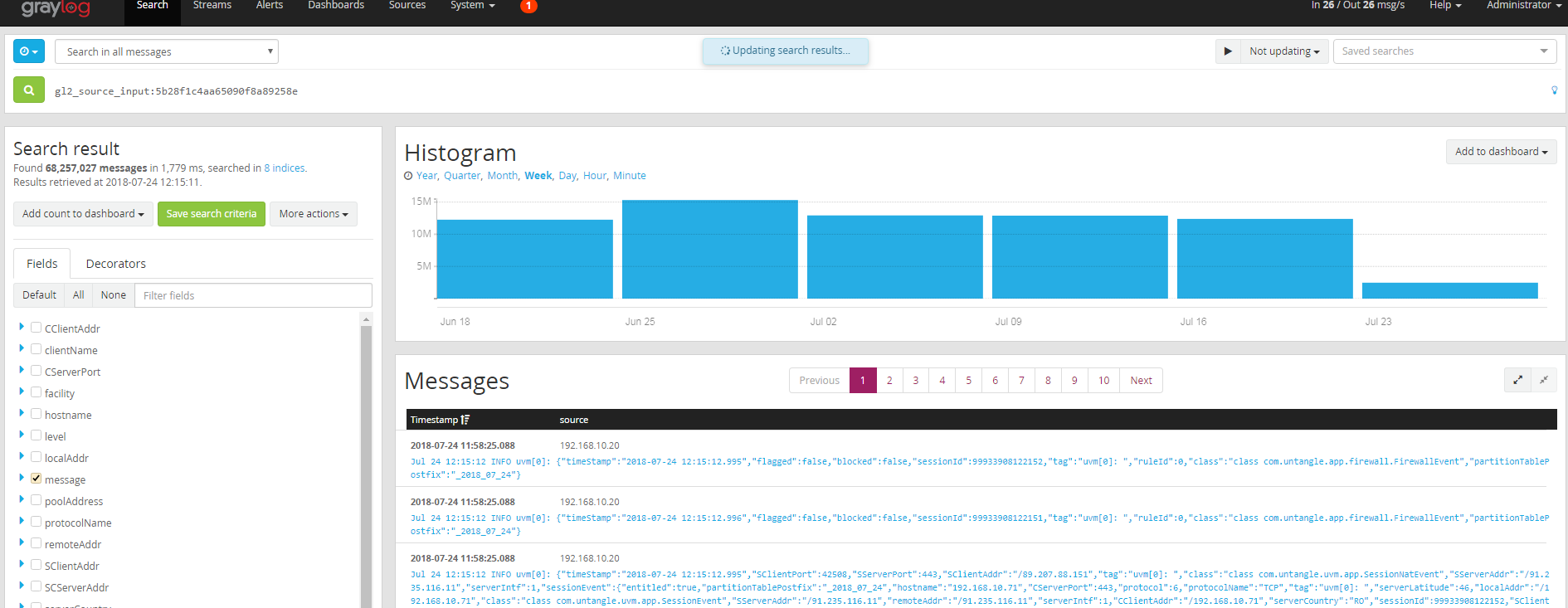
Важно: Порты назначаются не ниже 1025



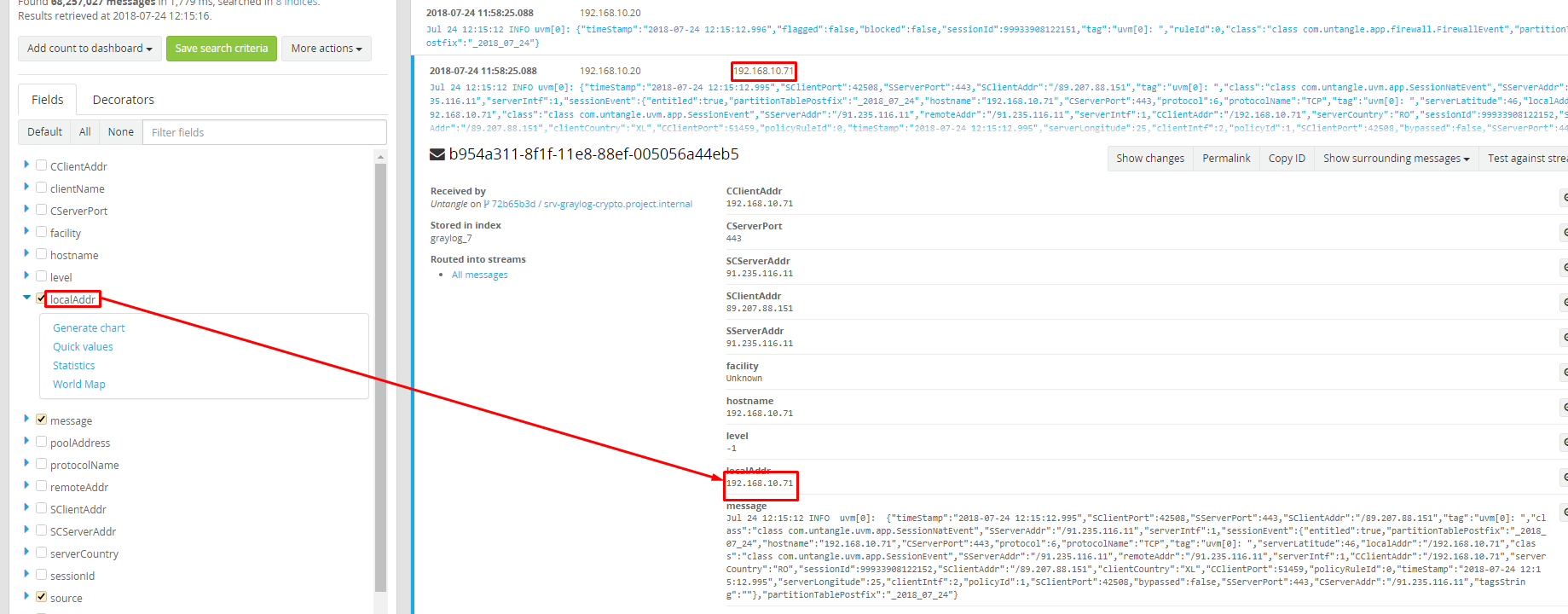
Тут видим информацию о поступающих логах



Переходим в просмотр поступающих логов



Здесь мы можем делать все теже действия что в П.1 Search только по конкретному источнику(inputs)

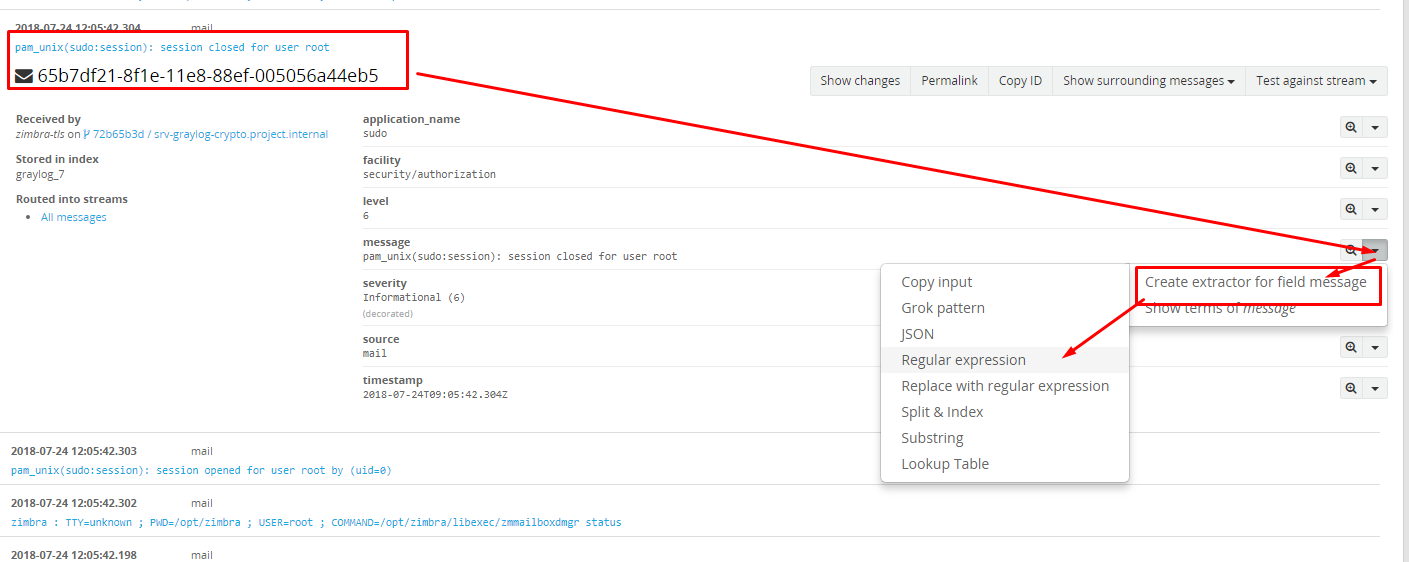


Сортировать информацию по полям и т.п. действия

1. Добавить поле или парсинг сообщения

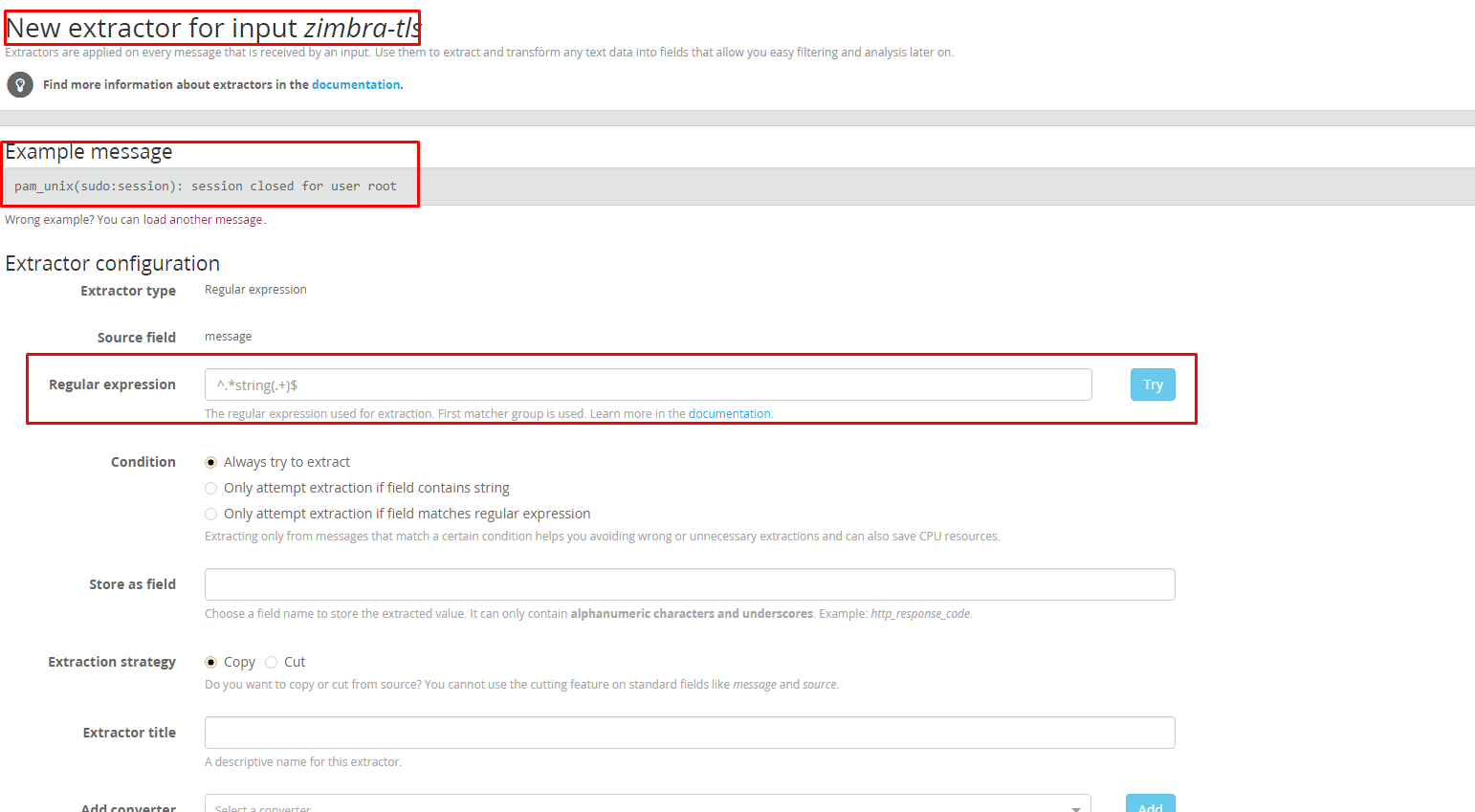
Раскрываем сообщение, выбираем сообщение которые будет разбирать в данном случае message

Далее Create extractor for field message > Regular expression



Переходим в создание нового поля с помощью регулярного сообщения. Тут видим

Для какого inputs делает поле, пример сообщения и поля для правил сообщения.



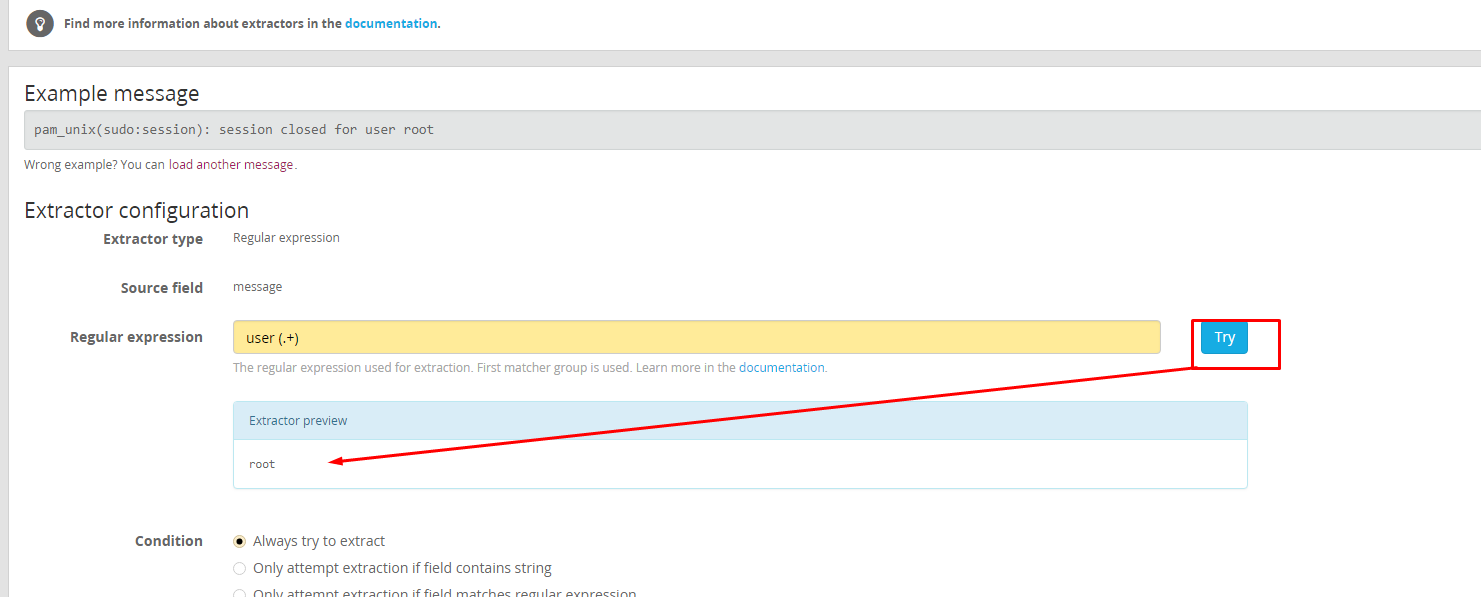
В данном случае хотим получить имя пользователя, завершившего сессию.

Вот так выглядит сообщение pam\_unix(sudo:session): session closed for user root

Нужно выделить имя, тут все просто если нет спец символов, определяем шаблон

В Regular expression user (.+)

Это значит что будет взята и выделена строка после user, жмем try получаем результат



Если нас результат устраивает сохраняем его.

Заполняем название поля и название заголовка поля

