Spis treści

Wprowadzenie 2
Opis podstawowych elementów systemu Graylog 2
Input 3
Extractors 4
Streams 5
Output 5
Alerts 5
Alerts overview 5
Notifications 6
Dashboards 7
Geolocation 8
Pipelines 9
Rules 9
Zadania 10

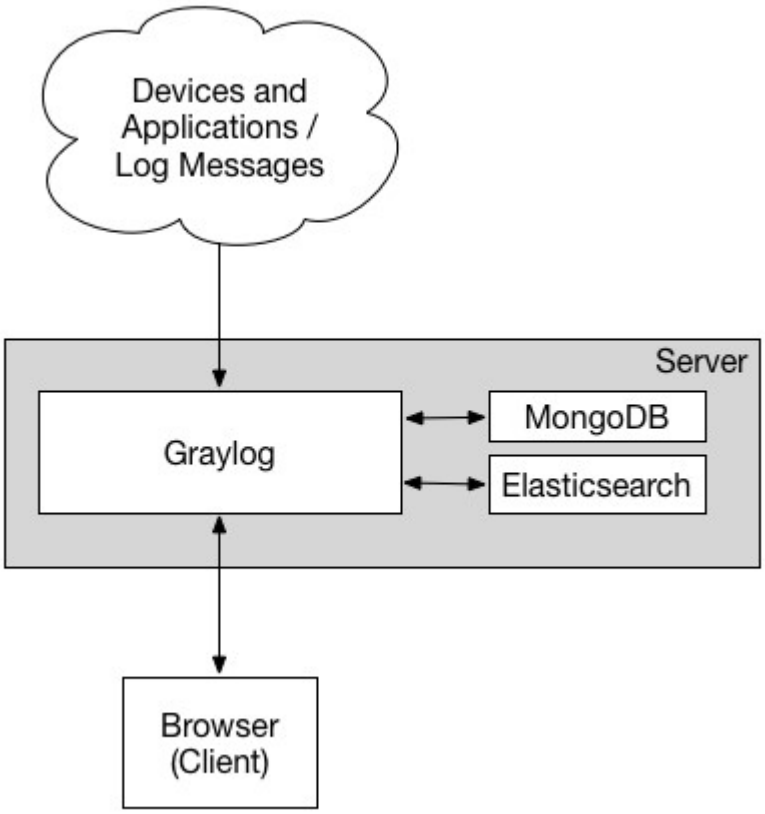
Wprowadzenie

Monitorowanie systemów teleinformatycznych, w związku z ich rozwojem i dużą popularnością, staje się aktualnie wyzwaniem, któremu trzeba sprostać. Obecnie, nie jest już wystarczające monitorowanie poszczególnych komponentów czy sieci, a istotne incydenty rzutują na kilka komponentów naszego systemu równocześnie. Jedynie kompleksowa analiza logów, z wszystkich elementów sieci pozwala na okrycie przyczyn i skutków nieoczekiwanych zdarzeń.

Przedmiotem zajęć jest konfiguracja centralnego systemu zbierania i analizy logów przy pomocy narzędzie Graylog.

Opis podstawowych elementów systemu Graylog

Graylog jest bardzo elastycznym rozwiązaniem pozwalającym na agregację i analizę logów pochodzących z różnych źródeł. Na potrzeby laboratorium przygotowane zostało środowisko w wersji minimalistycznej - wszystkie komponenty uruchomione na tej samej maszynie. W środowisku produkcyjnym, w zależności od potrzeb, mogą zostać one rozdzielne.

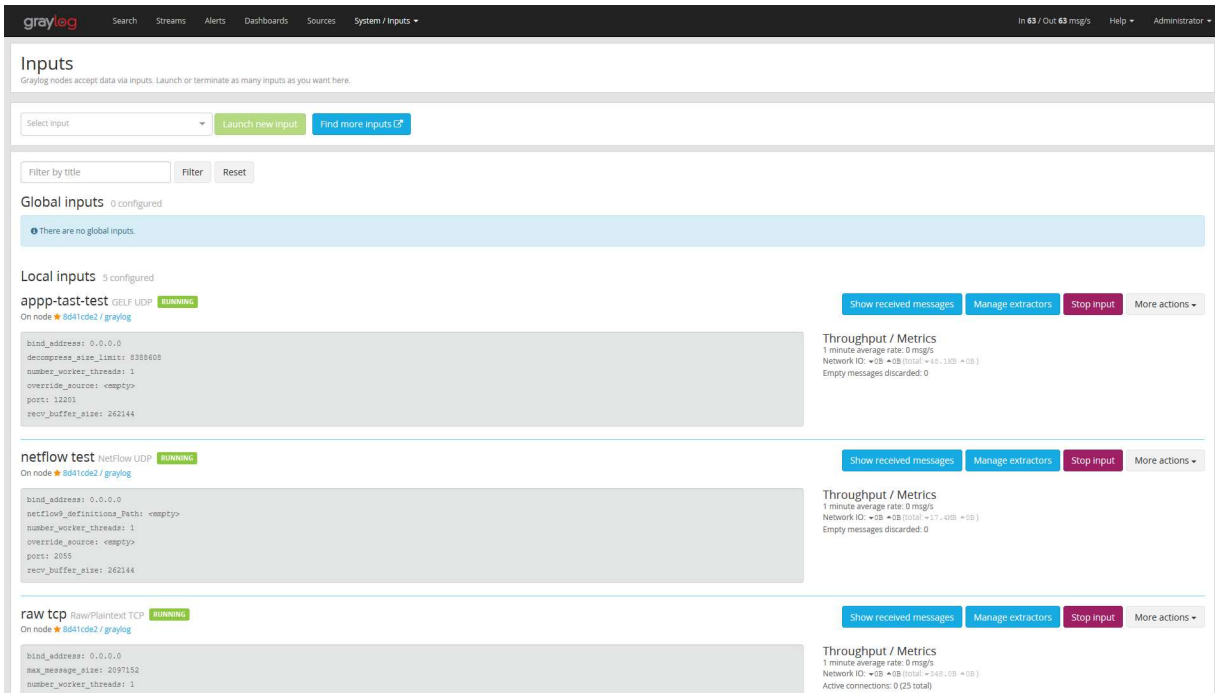


Input

pełna dokumentacja http://docs.graylog.org/en/3.0/pages/sending_data.html#what-are-graylog-message-inputs

Źródła komunikatów (Inputs) to elementy systemu Graylog odpowiedzialne za przyjmowanie logów, wiadomości o zdarzeniach. Są one uruchamiane z interfejsu WWW (lub API REST) w sekcji *System -> Inputs*. Ich utworzenie, uruchomienie, modyfikacja konfiguracji nie wymaga ponownego uruchomienia całego systemu. W domyślnej konfiguracji system umożliwiają odbieranie wiadomości różnego typu, zgodnie z poniższą listą, która może zostać rozszerzona o wejścia definiowane przez pluginy.

- Syslog (TCP, UDP, AMQP, Kafka)
- GELF(TCP, UDP, AMQP, Kafka, HTTP)
- AWS - AWS Logs, FlowLogs, CloudTrail
- Beats/Logstash
- CEF (TCP, UDP, AMQP, Kafka)
- JSON Path from HTTP API
- Netflow (UDP)
- Plain/Raw Text (TCP, UDP, AMQP, Kafka)

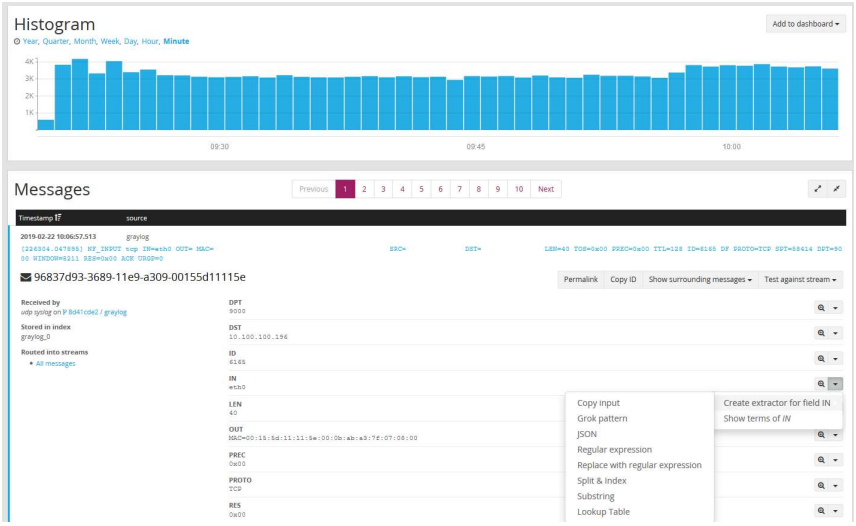


Extractors

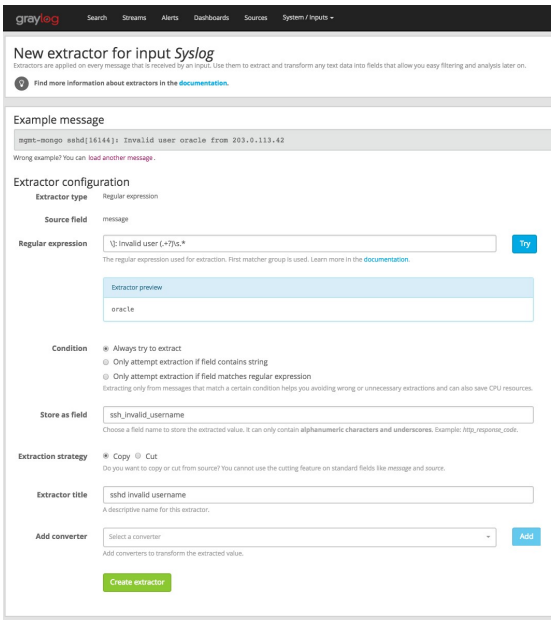
pełna dokumentacja: http://docs.graylog.org/en/3.0/pages/extractors.html

Niestety istnieje wiele urządzeń i aplikacji, które wysyłają logi przypominające format syslog, ale w rzeczywistości łamią zasady określone w RFC. W związku z czym przygotowanie predefiniowanych schematów pozwalających na czytanie i prawidłową interpretacje danych nie byłoby efektywne. W systemie Graylog pozostawiono możliwość definiowana reguł nazywanych Ekstraktorami. Ekstraktory pozwalają wyodrębnienie danych z dowolnego tekstu w otrzymanej wiadomości i rozszerzenie wiadomości o nowe pola z wyodrębnionymi danymi.

Ekstraktory dodawane są do wejścia strumienia poprzez wybór pozycji *Manage extractors* z menu po prawej stronie albo poprzez dodanie ekstraktora dla konkretnego pola po rozwinięciu wiadomości, tak jak to zaprezentowano na poniższej ilustracji:



W zależności od wybranego typu ekstraktora należy zdefiniować reguły filtrowania pola, które można przetestować klikając na przycisk *Try*.



Streams

pełna dokumentacja http://docs.graylog.org/en/3.0/pages/streams.html

Strumienie Graylog są mechanizmem umożliwiającym przekierowywanie wiadomości do zdefiniowanej przez użytkownika kategorii w czasie ich przetwarzania. Użytkownik definiuje reguły, które wskazują, które wiadomości mają być przekierowywane do strumienia. Przykładowym zastosowaniem strumieni jest utworzenie strumienia, który wychwytuje każdy komunikat o błędzie z określonego wejścia (*Input*). Wiadomość może być częścią wielu strumieni, a nie tylko jednego, a przypisanie do strumienia odbywa się na zasadzie dopasowania reguł.

Analiza strumieni w czasie rzeczywistym, pozwala to na ostrzeganie i przekazywanie wiadomości do innych systemów również w czasie rzeczywistym.

Output

Wyjścia strumienia umożliwia przekierowanie każdej wiadomości, która jest przetwarzana w ramach strumienia do innych systemów.

Wyjścia są zarządzane globalnie, a nie dla pojedynczych strumieni. Można konfigurować nowe wyjścia i aktywować je dla dowolnej liczby strumieni.

Graylog jest dostarczany z domyślnymi wyjściami i może być rozszerzony o Plugins.

Alerts

W obrębie strumienia, można zdefiniować warunki, które wyzwalają alarm. Na przykład, gdy konkretny strumień ma więcej niż 50 komunikatów na minutę lub gdy pole z określoną wartością ma zbyt duże odchylenie standardowe w ciągu ostatnich pięciu minut. Każdy alarm może znajdować się w jednym z dwóch stanów:

Unresolved Alert

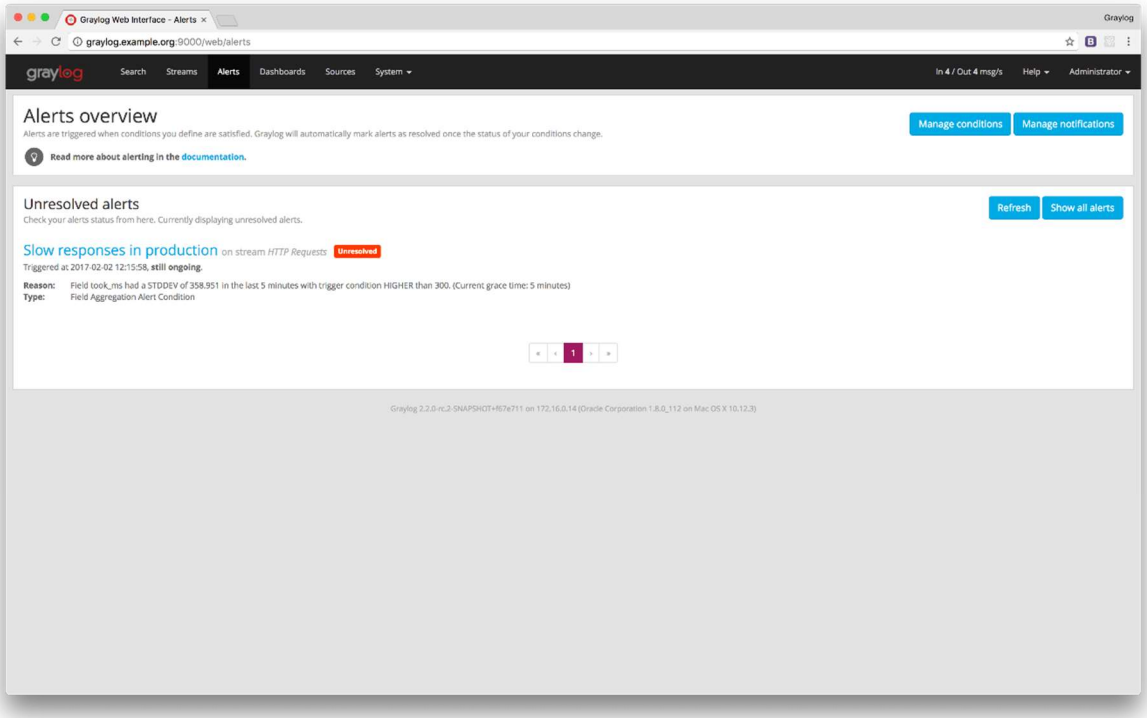
Alerty mają stan Unresolved Alert, gdy spełniony jest określony w nich warunek. W tym stanie wyzwalane są nowe alerty, a także wykonywane są powiadomienia dołączone do strumienia.

Resolved Alert

Graylog automatycznie zmienia stan alarmu na Resolved Alert, gdy jego warunek nie jest już spełniony. Jest to ostateczny stan alertu, a Graylog utworzy nowy alert, jeśli stan alarmu zostanie ponownie spełniony w przyszłości. Po zmianie stanu alarmu zastosowany zostanie okres prolongaty zdefiniowany w definicji alarmu.

Alerts overview

Strona przeglądowa alarmów pozwala w łatwy sposób dowiedzieć się, które alerty obecnie wymagają uwagi użytkownika, a jednocześnie umożliwia sprawdzenie alertów, które zostały wyzwolone w przeszłości i są teraz rozwiązane.



Notifications

Powiadomienia, przy wyzwoleniu alarmu, umożliwiają przesyłanie informacji do innych systemów. Sposób powiadamiania powinien być odpowiednio skonfigurowany w zależności od wykorzystywanego systemu (wysłanie wiadomości e-mail, SMS, żądania HTTP).

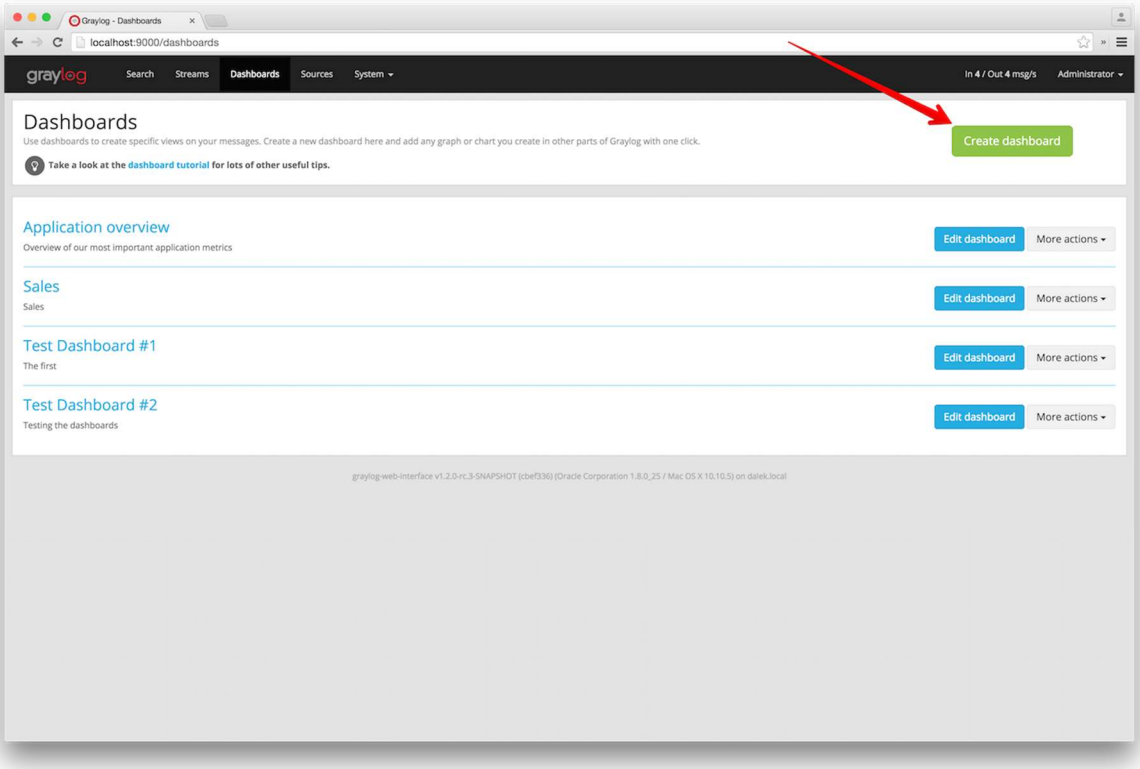
Dashboards

pełna dokumentacja http://docs.graylog.org/en/3.0/pages/dashboards.html

Korzystanie z elementów dashboard pozwala na budowanie predefiniowanych widoków prezentujących w wybrany sposób gromadzone dane. Na podstawie dostępnych widgetów można dodawać aktywne (dynamiczne) komponenty prezentujące np. dane geolokalizacyjne, wykresy, wartości liczbowe z wskazaniem trendu ich zmiany.

Tworzenie nowego Dashboard

W sekcji *Dashboards*, system prezentuję listę wszystkich elementów dashboard, które możesz przeglądać. Przycisk *Create dashboard* pozwala utworzyć nowy element. Na tym etapie, jedyną wymaganą informacją jest tytuł i opis nowego elementu dashboard.



Do elementu Dashboard można dodać następujące typy wyników wyszukiwania:

- Search result counts
- Search result histogram charts
- Statistical values
- Field value charts
- Stacked charts
- Quick values results

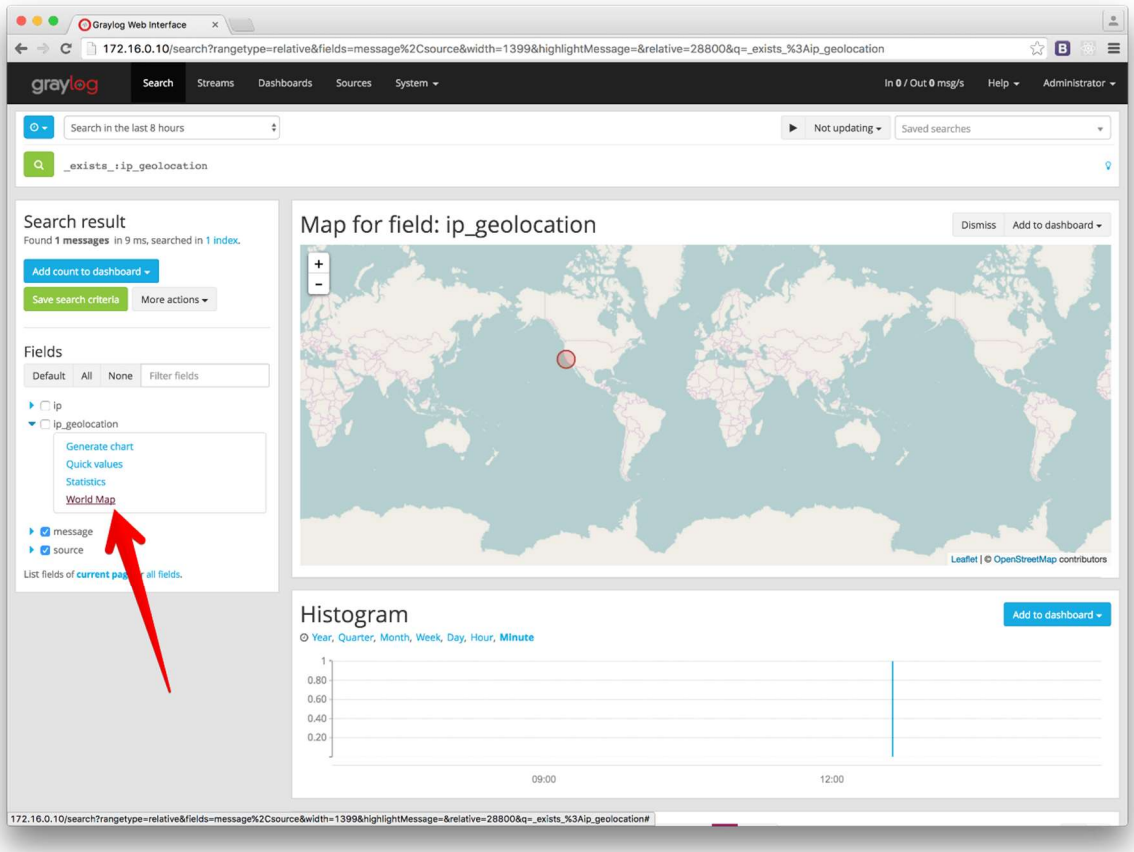
Dodanie odpowiedniego komponentu możliwe jest z poziomu widoku prezentującego zgromadzone wiadomości. Wybór sposobu analizy i prezentacji danych dla konkretnego parametru dodaje element do aktualnego widoku – element ten następnie może być dodany do wybranego Dashboard.

Geolocation

pełna dokumentacja: http://docs.graylog.org/en/3.0/pages/geolocation.html

Graylog może wyświetlać mapy z geolokalizacji przechowywane w dowolnym polu, o ile punkty geolokalizacyjne wykorzystują format szerokości i długości geograficznej. Domyślna wartość zwracana przez Geo IP Data Adapter zwraca współrzędne w odpowiednim formacie.

Na dowolnej stronie wyników wyszukiwania można rozszerzyć pole, aby narysować mapę w pasku bocznym wyszukiwania, a następnie kliknąć na link *World Map*. Wyświetli się mapa z wszystkimi punktami zapisanymi w tym polu. Po kliknięciu na przycisk *Add to dashboard* mapa zostanie umieszczona w odpowiednim elemencie Dashboard.



Pipelines

pełna dokumentacja: http://docs.graylog.org/en/3.0/pages/pipelines/pipelines.html

Pipeline zawierają reguły przetwarzania (*Rules*) i mogą być podłączone do jednego lub więcej strumieni danych wejściowych, umożliwiając precyzyjną kontrolę przetwarzania komunikatów. Reguły przetwarzania to po prostu warunki, po których następuje lista działań, ale nie oferują one kontroli przepływu. Taką możliwość wprowadzono w etapach, które należy traktować jako grupy warunków i działań wykonywanych w określonej kolejności. Wszystkie etapy o tym samym priorytecie przebiegają w tym samym czasie przez wszystkie połączone elementy pipeline.

Etapy są prowadzone w kolejności określonej przez priorytet. Priorytetami etapów mogą być dowolne liczby całkowite(zarówno dodatnie, jak i ujemne).

Reguły są identyfikowane przez nazwy i mogą być współdzielone pomiędzy wiele różnych elementów pipeline. Celem jest umożliwienie tworzenia bloków wielokrotnego użytku, co ułatwi przetwarzanie specyficznych danych.

Rules

pełna dokumentacja: http://docs.graylog.org/en/3.0/pages/pipelines/rules.html

Reguły pozwalają na rozszerzone (względem ekstraktorów) przetwarzanie wiadomości. Aby uniknąć złożoności całego języka programowania, w systemie Graylog zaimplementowany uproszczony język reguł wykorzystywany do określenia logiki przetwarzania. Język reguł jest celowo ograniczony, aby umożliwić łatwiejsze zrozumienie, szybszą jego naukę i lepszą optymalizację czasu pracy.

Prawdziwa praca reguł jest wykonywana w funkcjach, które są rozszerzalne przez pluginy. Graylog jest już dostarczany z dużą ilością wbudowanych funkcji, zapewniających np. konwersję danych, manipulację łańcuchami czy parsowanie JSON.