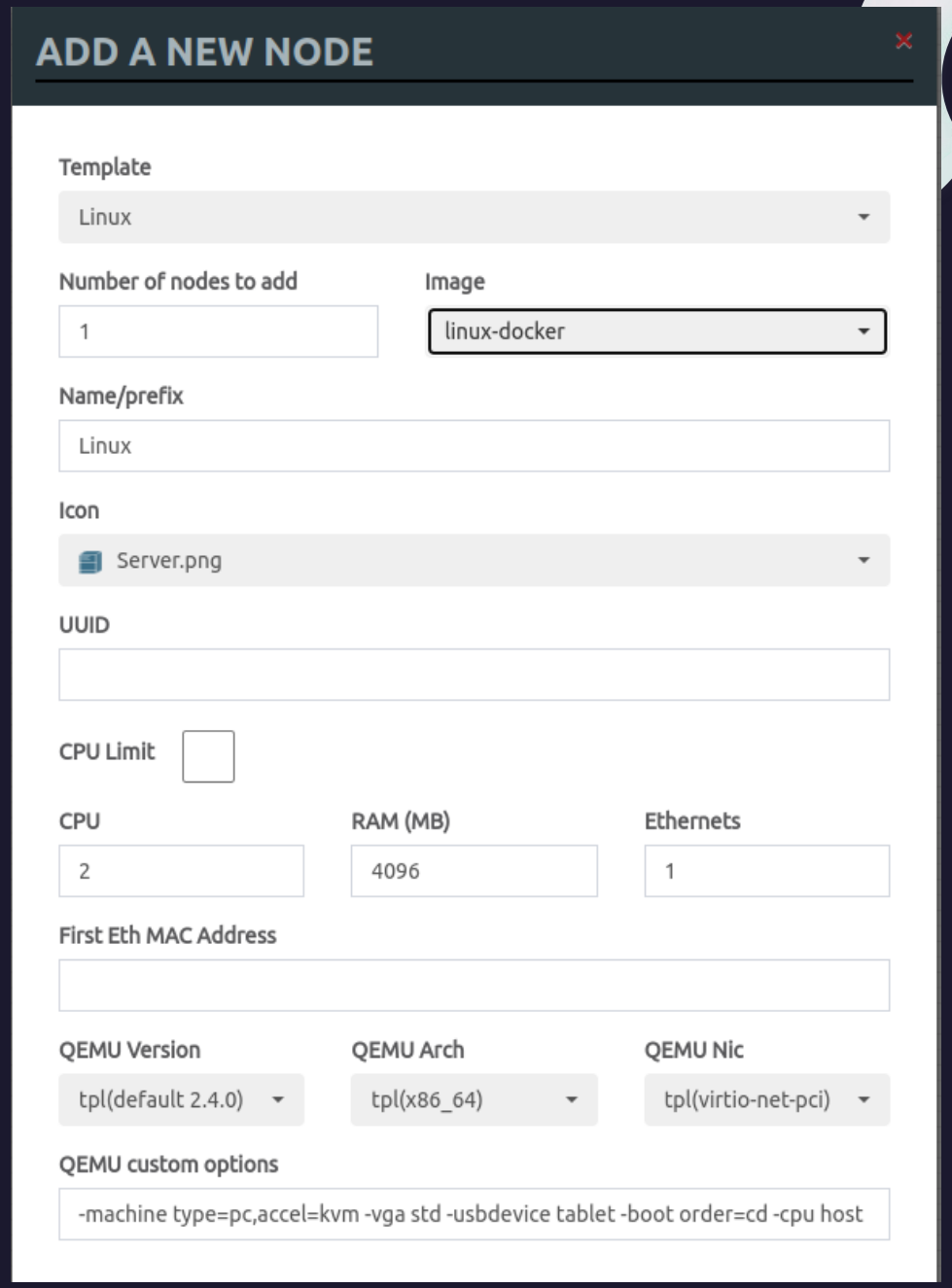
Laboratoare Administarea Retelelor de Calculatoare

Event management cu Elasticsearch/Opensearch si Graylog.

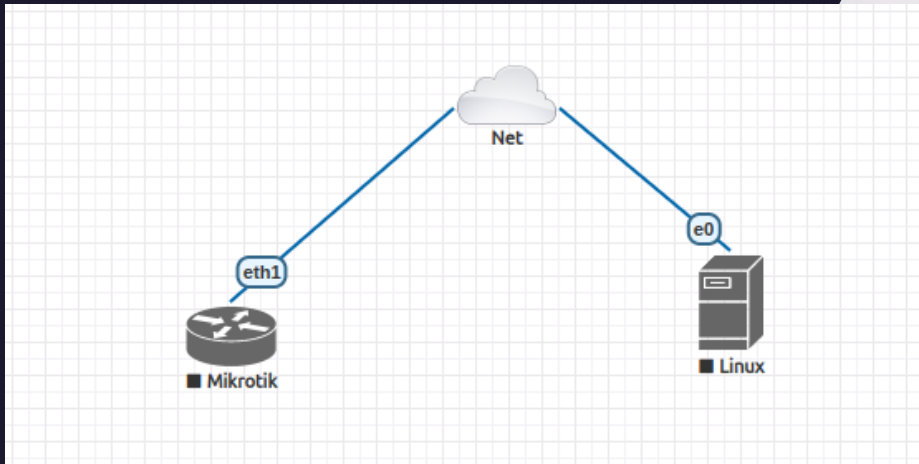
Setup-ul initial

- Incepem prin a instala serverul de Graylog.
- In acest laborator il vom instala in docker prin imaginea de eve facuta de mine si accesibila la urmatorul link: [linux docker image](#).
- Copiem imaginea in serverul eve in calea: "/opt/unetlab/addons/qemu" unde facem un folder numit linux-docker, dupa care o redenumim in virtioa.qcow2.
- Rulam scriptul unl unl_wrapper -a fixpermissions
- Acum putem adauga serverul in laborator.
  - Trebuie sa ne asiguram ca avem in QEMU custom options optiunea "-cpu host" in cazul in care nu exista trebuie adaugat la sfarsitul stringului existent.



Setup-ul initial

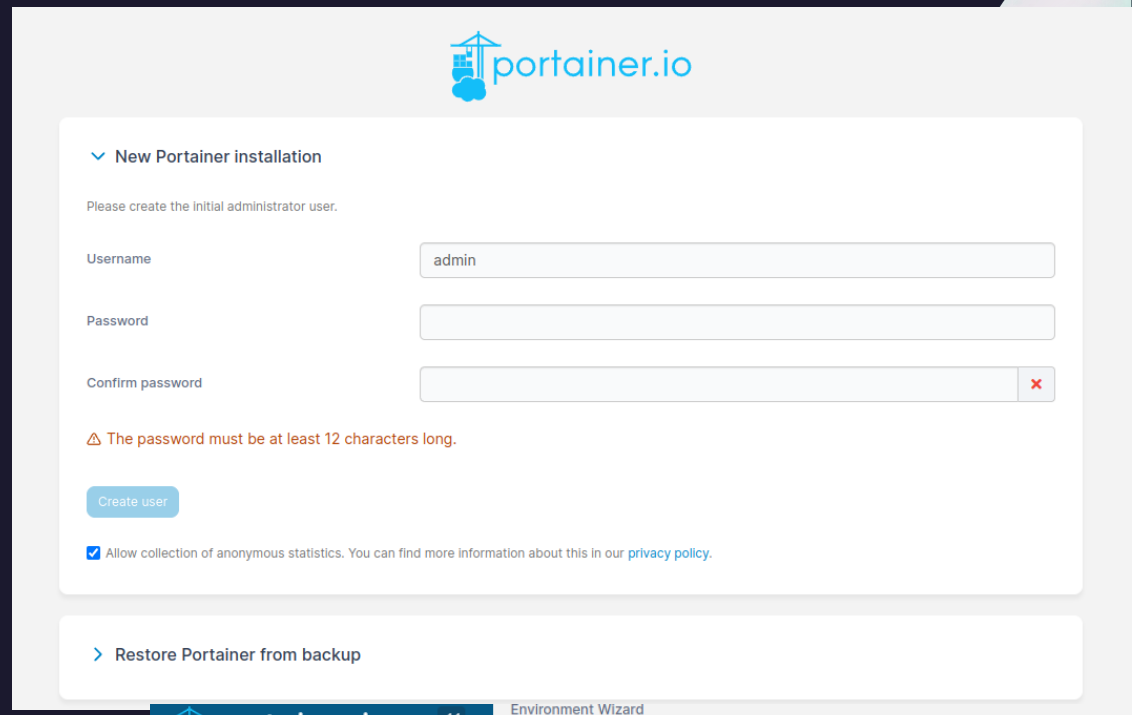
- Se poate instala si un server virtual separat si configurat sau orice alta metoda care duce la instalarea acestui server, calea aleasa de mine este cea mai suoara varianta de instalare in laboratorul virtual.
- Punem si un router Mikrotik legeat la internet impreuna cu serverul nostru si pornim serverul.
- Credentialele default sunt username: root si parola: eve.
- Dupa ce intram in server verificam ce ip are si ne conectam pe interfata https://<ip>:9443

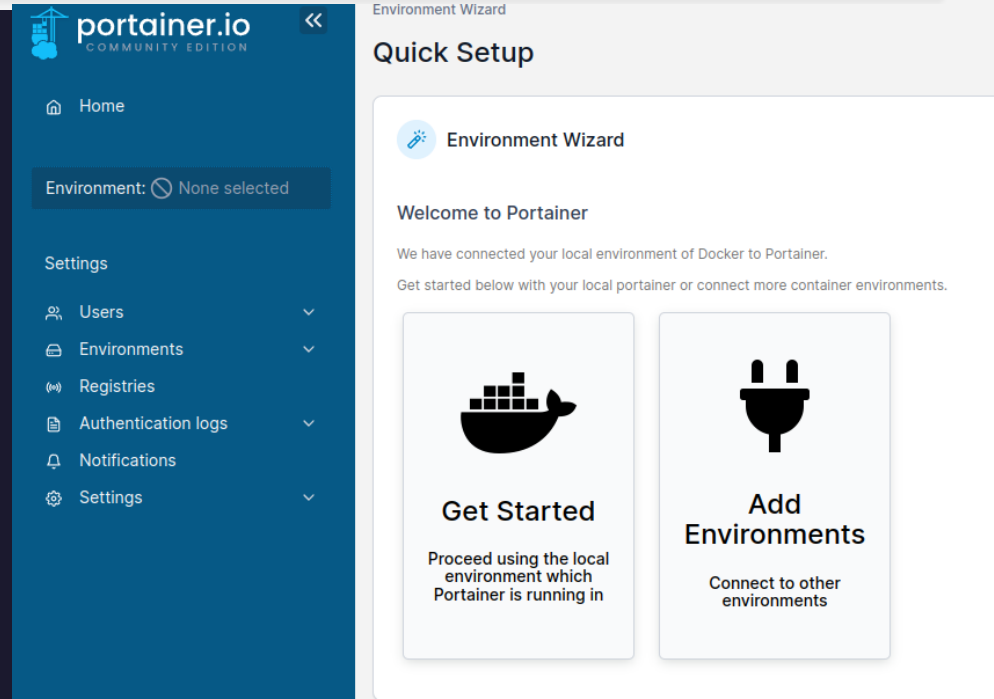


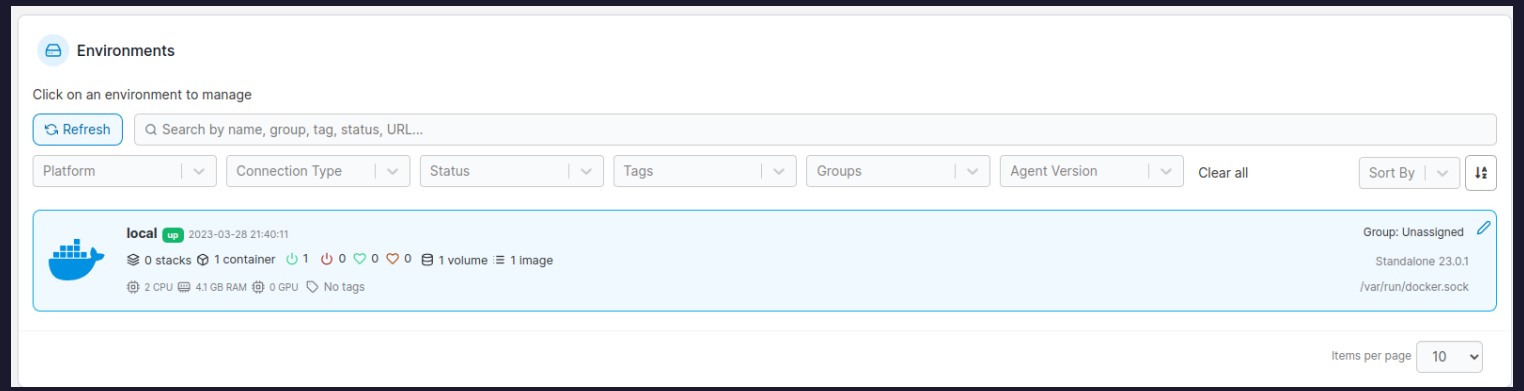

```
[root@docker ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:00:00:02:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.122.234/24 brd 192.168.122.255 scope global dynamic noprefixroute ens3
       valid_lft 3405sec preferred_lft 3405sec
    inet6 fe80::ab79:1b69:5b19:8e03/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:87:ee:92:e5 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:87ff:feee:92e5/64 scope link
       valid_lft forever preferred_lft forever
5: veth94ed7f2@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether a6:d2:03:d3:98:08 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::a4d2:3ff:fed3:9808/64 scope link
       valid_lft forever preferred_lft forever
[root@docker ~]#
```

Setup-ul initial

- Acum ca am ajuns la interfata de administrare ne setam parola.
- Apoi dam pe Get Started si vedem instanta locala preconfigurata.

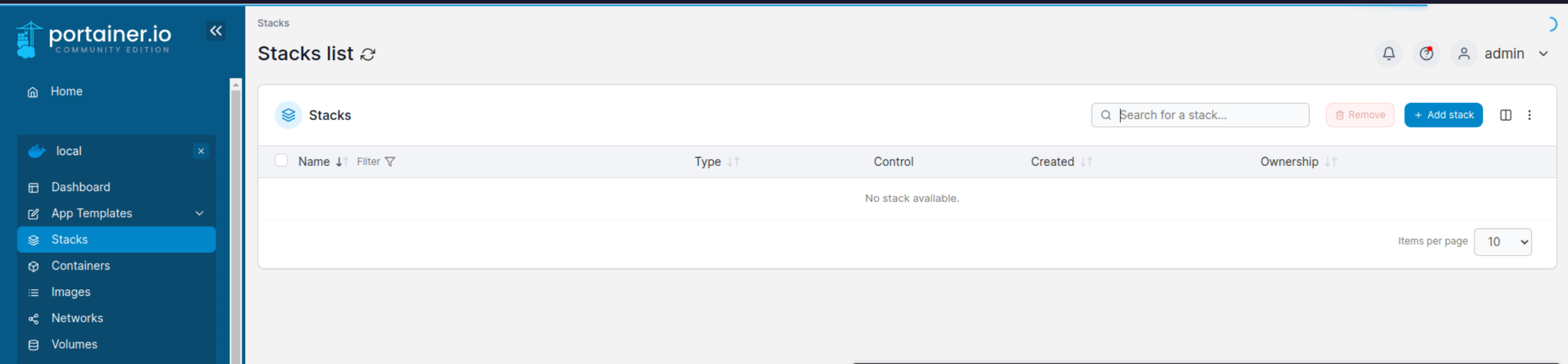






Instalarea Graylog

- Intam in Stacks care este defapt docker compose si configuram un script yaml apasand pe Add stack.
- Accesam link-ul cu fisierul de configuratie: [graylog docker compose file]() folosind acest config ca baza pentru instalarea noastra.



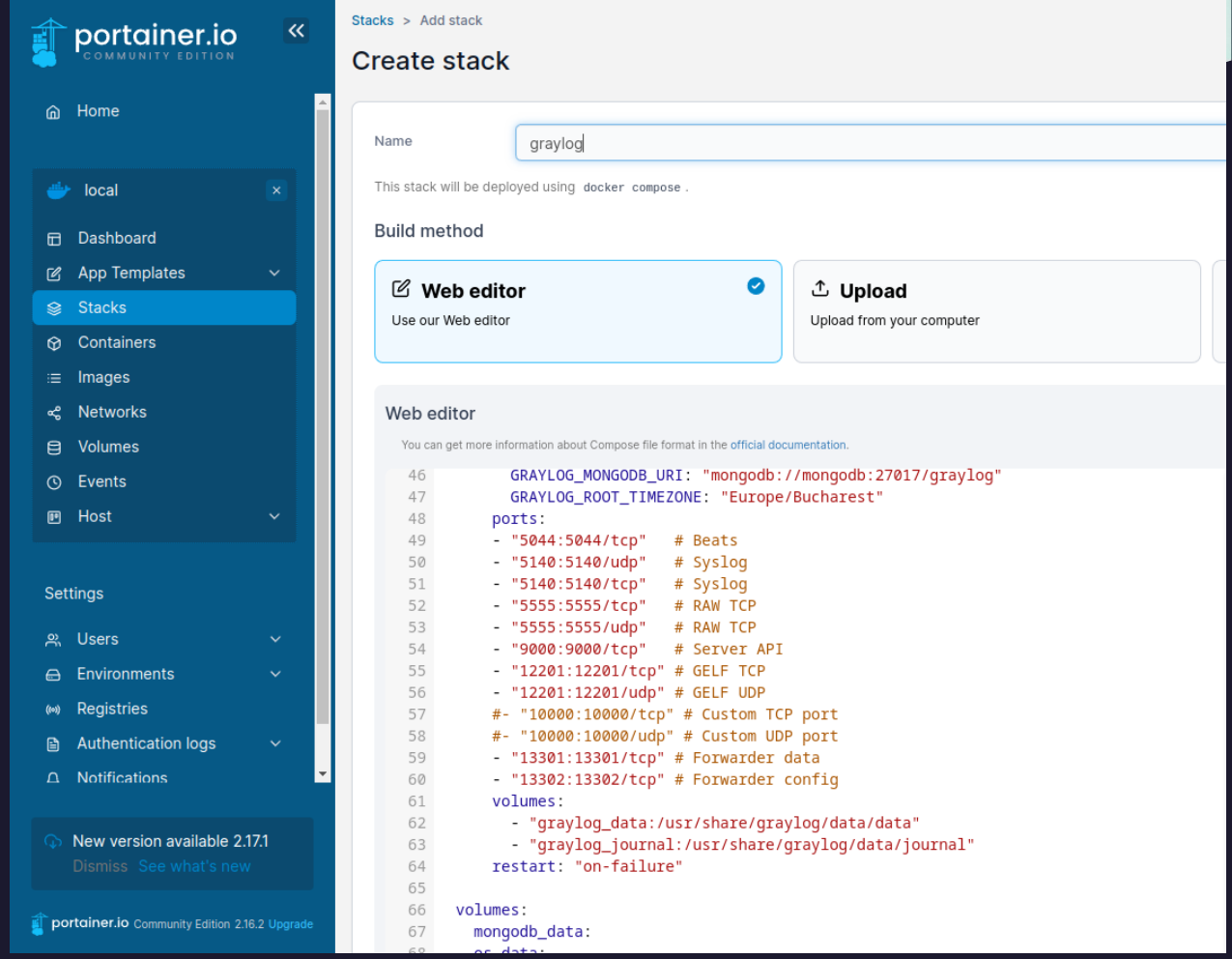
Instalarea Graylog

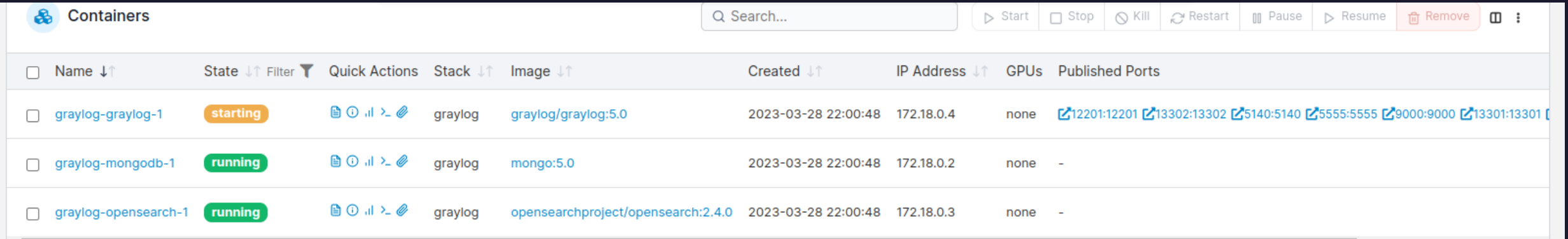
- Trebuie sa moficam in princiap 3 parametrii.
- GRAYLOG_PASSWORD_SECRET ruland comanda:
- “pwgen -N 1 -s 96”
- GRAYLOG_ROOT_PASSWORD_SHA2
- “echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1”
- GRAYLOG_ROOT_TIMEZONE:“Europe/Bucharest”

```
version: "3.8"

services:
  mongodb:
    image: "mongo:5.0"
    volumes:
      - "mongodb_data:/data/db"
    restart: "on-failure"

  opensearch:
    image: "opensearchproject/opensearch:2.4.0"
    environment:
      - "OPENSEARCH_JAVA_OPTS=-Xms1g -Xmx1g"
      - "bootstrap.memory_lock=true"
      - "discovery.type=single-node"
      - "action.auto_create_index=false"
      - "plugins.security.ssl.http.enabled=false"
      - "plugins.security.disabled=true"
    ulimits:
      memlock:
        hard: -1
        soft: -1
      nofile:
        soft: 65536
        hard: 65536
    volumes:
      - "os_data:/usr/share/opensearch/data"
    restart: "on-failure"

  graylog:
    hostname: "server"
    image: "${GRAYLOG_IMAGE:-graylog/graylog:5.0}"
    depends_on:
      opensearch:
        condition: "service_started"
      mongodb:
        condition: "service_started"
    entrypoint: "/usr/bin/tini -- wait-for-it opensearch:9200 --  /docker-entrypoint.sh"
    environment:
      GRAYLOG_NODE_ID_FILE: "/usr/share/graylog/data/config/node-id"
      GRAYLOG_PASSWORD_SECRET:
"7dgPW4OOVd8ISaajcQVy8hnESsXxd5Gj8omkmjWtp1N5BogTXr1Yy3HfGOqvlR2F0xOvcV8ppMm7pUnkJl9
ElmbMI7XhJO4w"
      GRAYLOG_ROOT_PASSWORD_SHA2:
"ecd71870d1963316a97e3ac3408c9835ad8cf0f3c1bc703527c30265534f75ae"
      GRAYLOG_HTTP_BIND_ADDRESS: "0.0.0.0:9000"
      GRAYLOG_HTTP_EXTERNAL_URI: "http://localhost:9000/"
      GRAYLOG_ELASTICSEARCH_HOSTS: "http://opensearch:9200"
      GRAYLOG_MONGODB_URI: "mongodb://mongodb:27017/graylog"
      GRAYLOG_ROOT_TIMEZONE: "Europe/Bucharest"
    ports:
    - "5044:5044/tcp"   # Beats
    - "5140:5140/udp"   # Syslog
    - "5140:5140/tcp"   # Syslog
    - "5555:5555/tcp"   # RAW TCP
    - "5555:5555/udp"   # RAW TCP
    - "9000:9000/tcp"   # Server API
    - "12201:12201/tcp" # GELF TCP
    - "12201:12201/udp" # GELF UDP
    #- "10000:10000/tcp" # Custom TCP port
    #- "10000:10000/udp" # Custom UDP port
    - "13301:13301/tcp" # Forwarder data
    - "13302:13302/tcp" # Forwarder config
    volumes:
      - "graylog_data:/usr/share/graylog/data/data"
      - "graylog_journal:/usr/share/graylog/data/journal"
    restart: "on-failure"

volumes:
  mongodb_data:
  os_data:
```

Instalarea Graylog

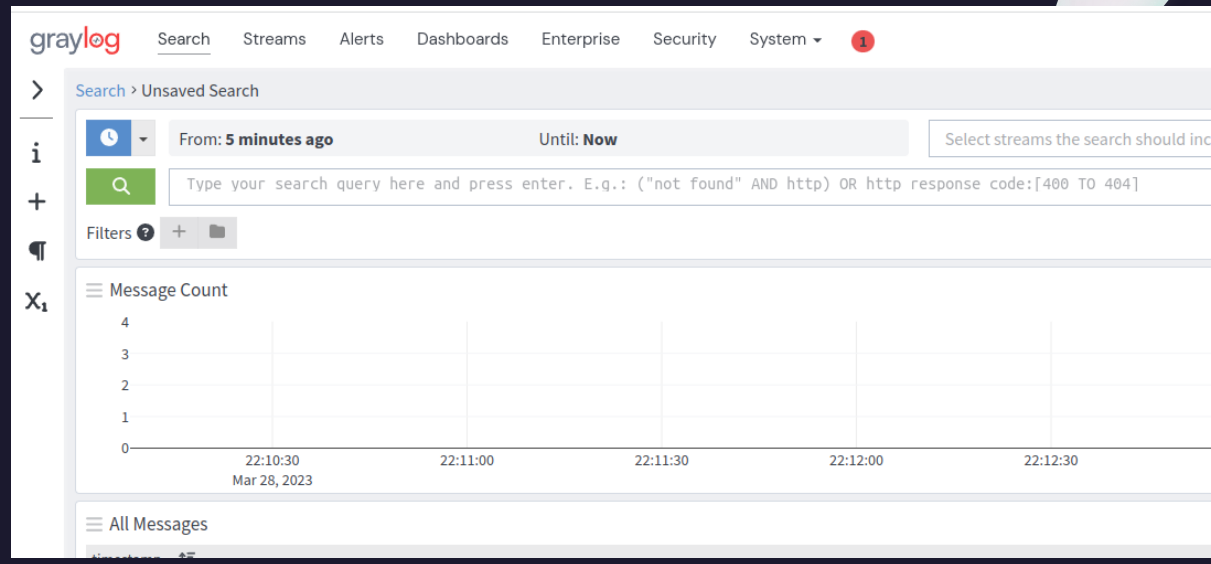
- Acum putem da “Deploy stack” si asteptam sa termine.
- Vedem ca au fost create 3 containere unu de opensearch, unul de mongodb si unul de graylog.





Instalarea Graylog

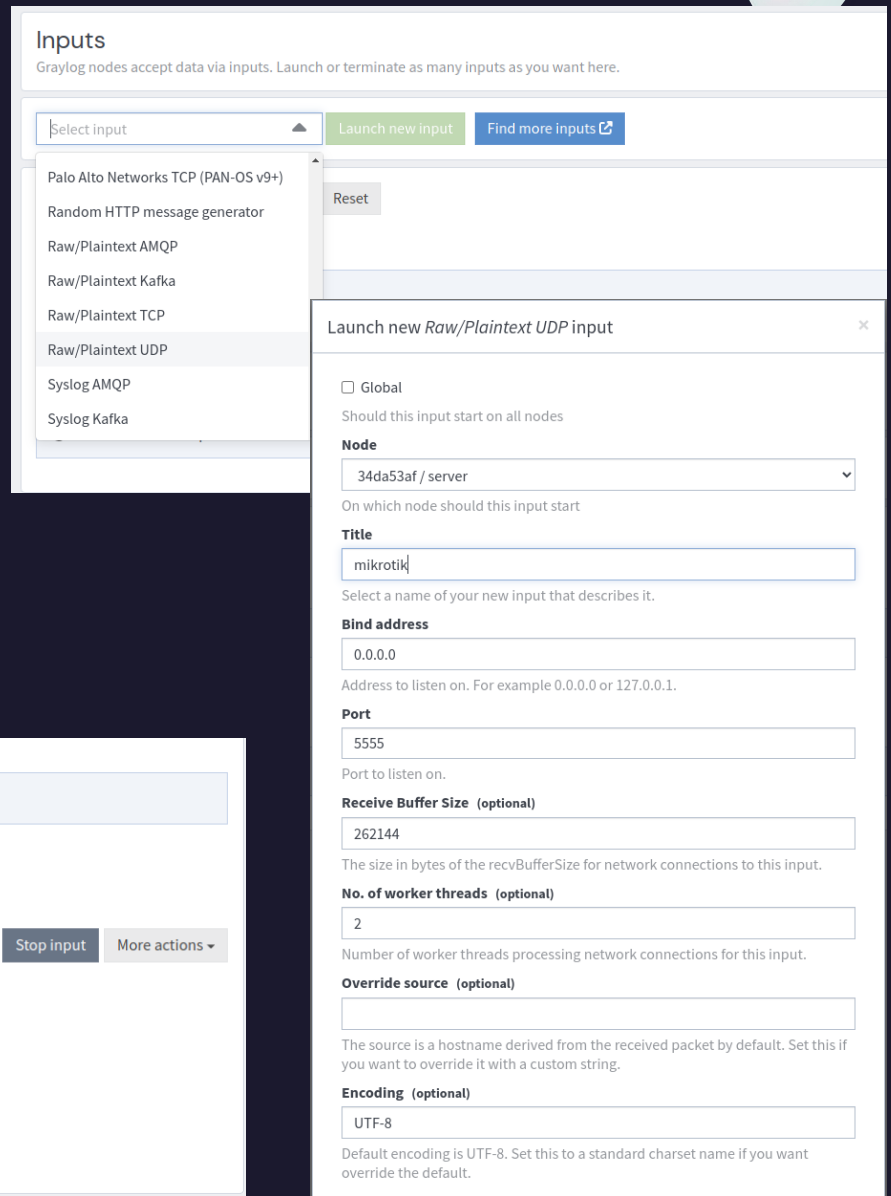
- In logurile de initializare ale containerului graylog putem vedea ca a pornit cu scucces si ne putem conecta la interfata web prin link-ul: http://<ip_docker>:9000
- Si folosind username-ul: “admin” si parola setata in config “GRAYLOG_ROOT_PASSWORD_SHA2”
- Putem vedea interfata din dreapta.

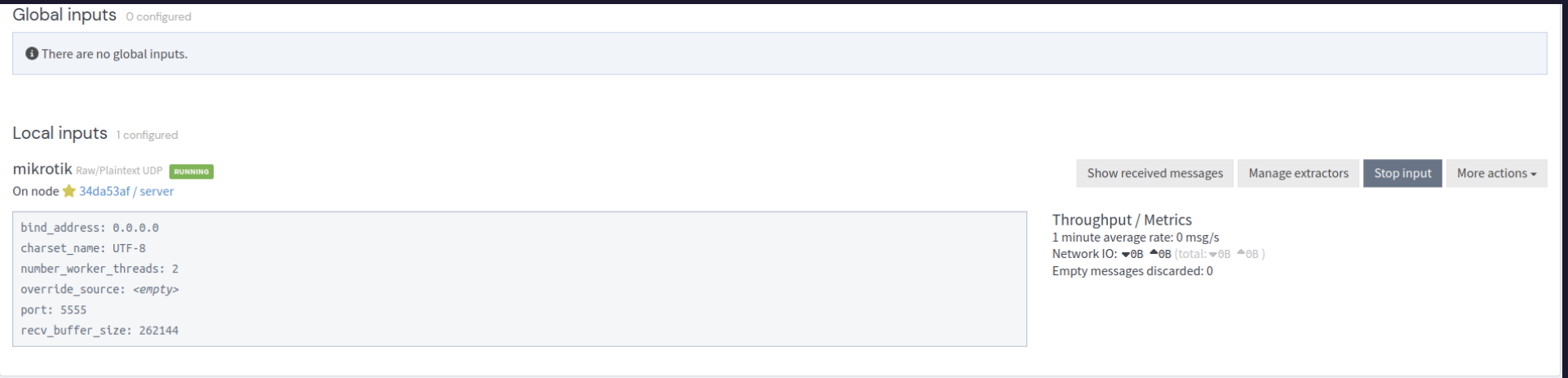



```
2023-03-28 19:01:46,245 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog2.indexer.fieldtypes.IndexFieldTypePollerP
2023-03-28 19:01:46,246 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.scheduler.periodicals.ScheduleTriggerClea
2023-03-28 19:01:46,246 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog2.periodical.ESVersionCheckPeriodical] per
2023-03-28 19:01:46,246 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog2.periodical.UserSessionTerminationPeriodi
2023-03-28 19:01:46,248 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.plugins.sidecar.periodical.PurgeExpiredSi
2023-03-28 19:01:46,248 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.plugins.sidecar.periodical.PurgeExpiredCo
2023-03-28 19:01:46,249 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.plugins.views.search.db.SearchesCleanUpJo
2023-03-28 19:01:46,250 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.events.periodicals.EventNotificationStatu
2023-03-28 19:01:46,250 INFO : org.graylog2.periodical.Periodicals - Starting [org.graylog.plugins.collector.periodical.PurgeExpired
2023-03-28 19:01:46,283 INFO : org.graylog2.security.UserSessionTerminationService - Globally terminated 0 session(s)
2023-03-28 19:01:46,535 INFO : org.graylog2.periodical.IndexRetentionThread - Elasticsearch cluster not available, skipping index re
2023-03-28 19:01:46,576 INFO : org.graylog2.indexer.MongoIndexSet - Did not find a deflector alias. Setting one up now.
2023-03-28 19:01:46,983 INFO : org.graylog2.indexer.MongoIndexSet - There is no index target to point to. Creating one now.
2023-03-28 19:01:47,022 INFO : org.graylog2.indexer.MongoIndexSet - Cycling from <none> to <graylog_0>.
2023-03-28 19:01:47,023 INFO : org.graylog2.indexer.MongoIndexSet - Creating target index <graylog_0>.
2023-03-28 19:01:48,424 INFO : org.graylog2.indexer.indices.Indices - Successfully ensured index template graylog-internal
2023-03-28 19:01:49,597 INFO : org.graylog2.shared.initializers.JerseyService - Started REST API at <0.0.0.0:9000>
```

Configurarea colecatorii de log-uri

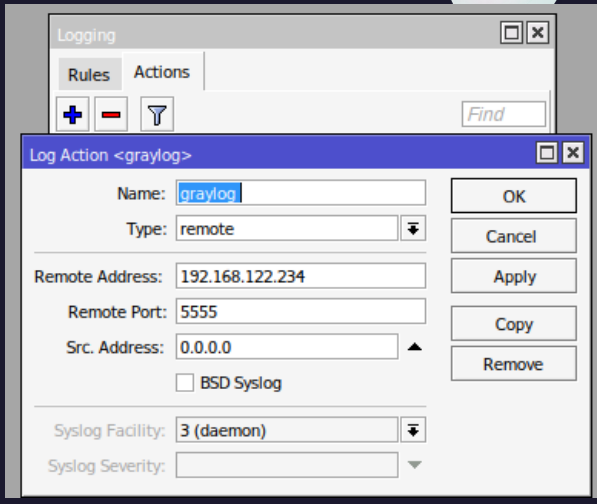
- Mergand in System→Inputs si configuram un nou input “Raw/Plaintext UDP” pentru ca este singurul mod in care mikrotik transmite logurile.
- Selecam un port care este mapat din container (ex: 5555).
- Acest input acctionaza ca un listener si primeste de la un client mesaje

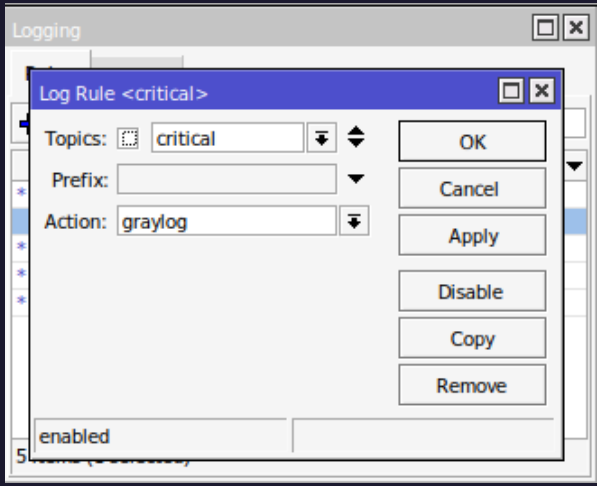




Configurarea colecatorii de log-uri

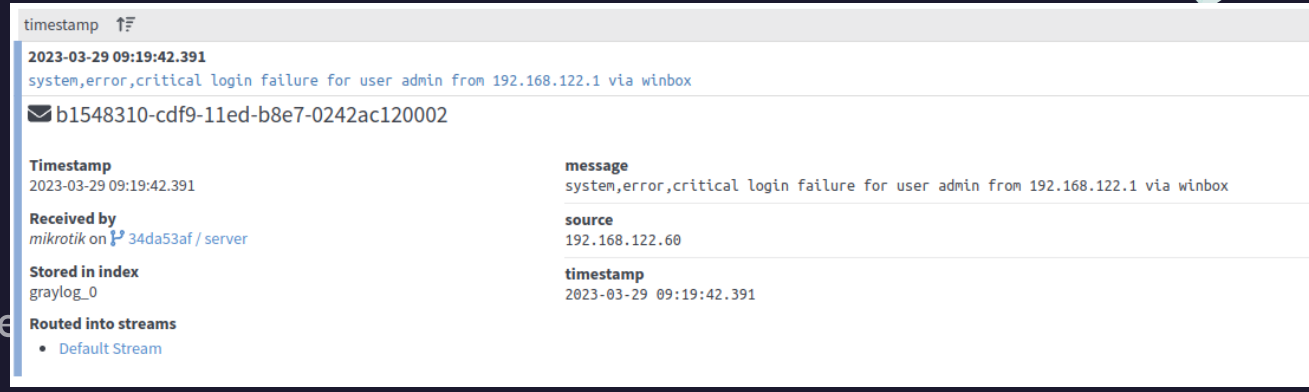
- Acum mergem pe router si configuram o noua destinatie pentru loguri mergand in System→Logging→Actions→+
- Avem setat un mod de a trimite logurile catre Graylog si putem selecta ce tipuri de loguri trimitem catre acesta.
- Putem incepe cu minotirzarea login fails asa ca vom face o regula noua in Logging.

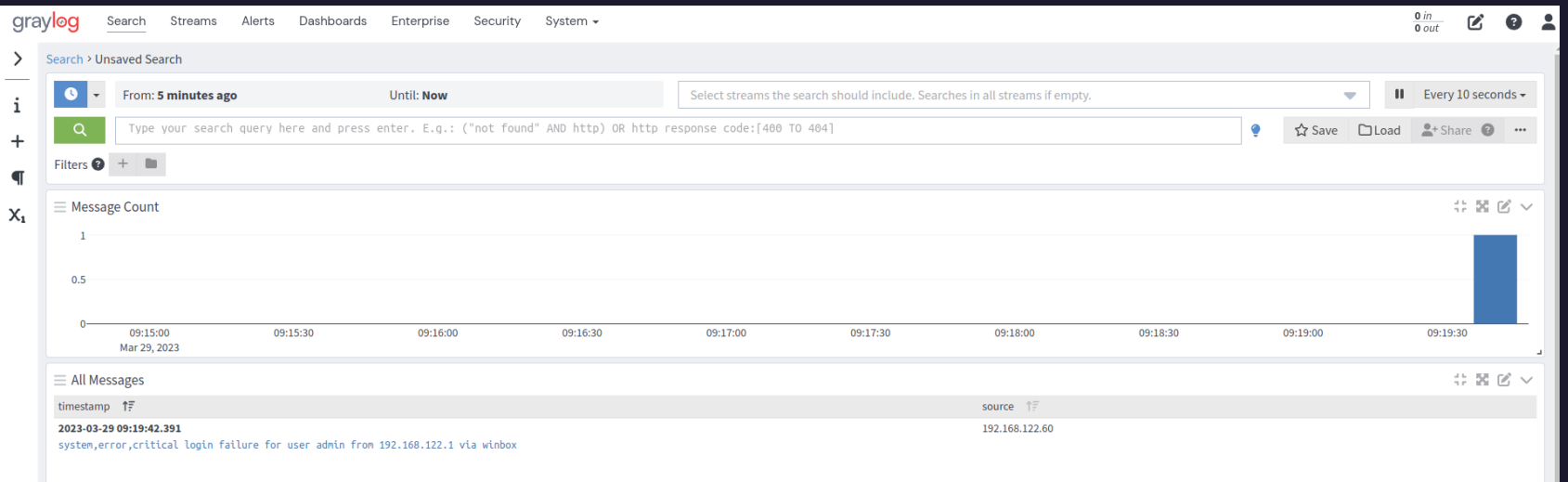




Configurarea colecatorii de log-uri

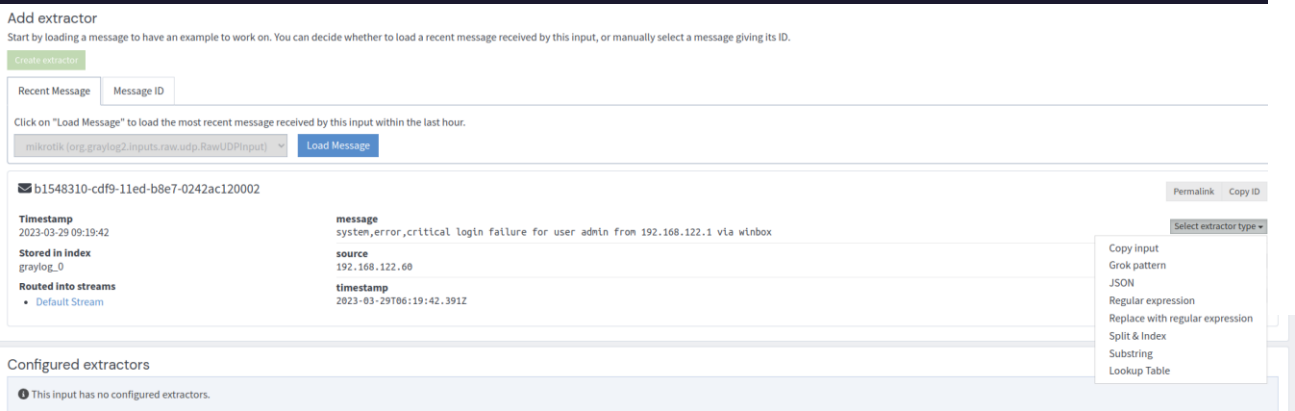
- Acum putem incerca un login fail pentru userul admin si vedea daca este transmis in graylog.
- Mergand la Search vedem o intrare in mesaje.
- Deschizand mesajul vedem ca acesta nu este procesat de graylog intr-o forma pe care el o poate intelege.

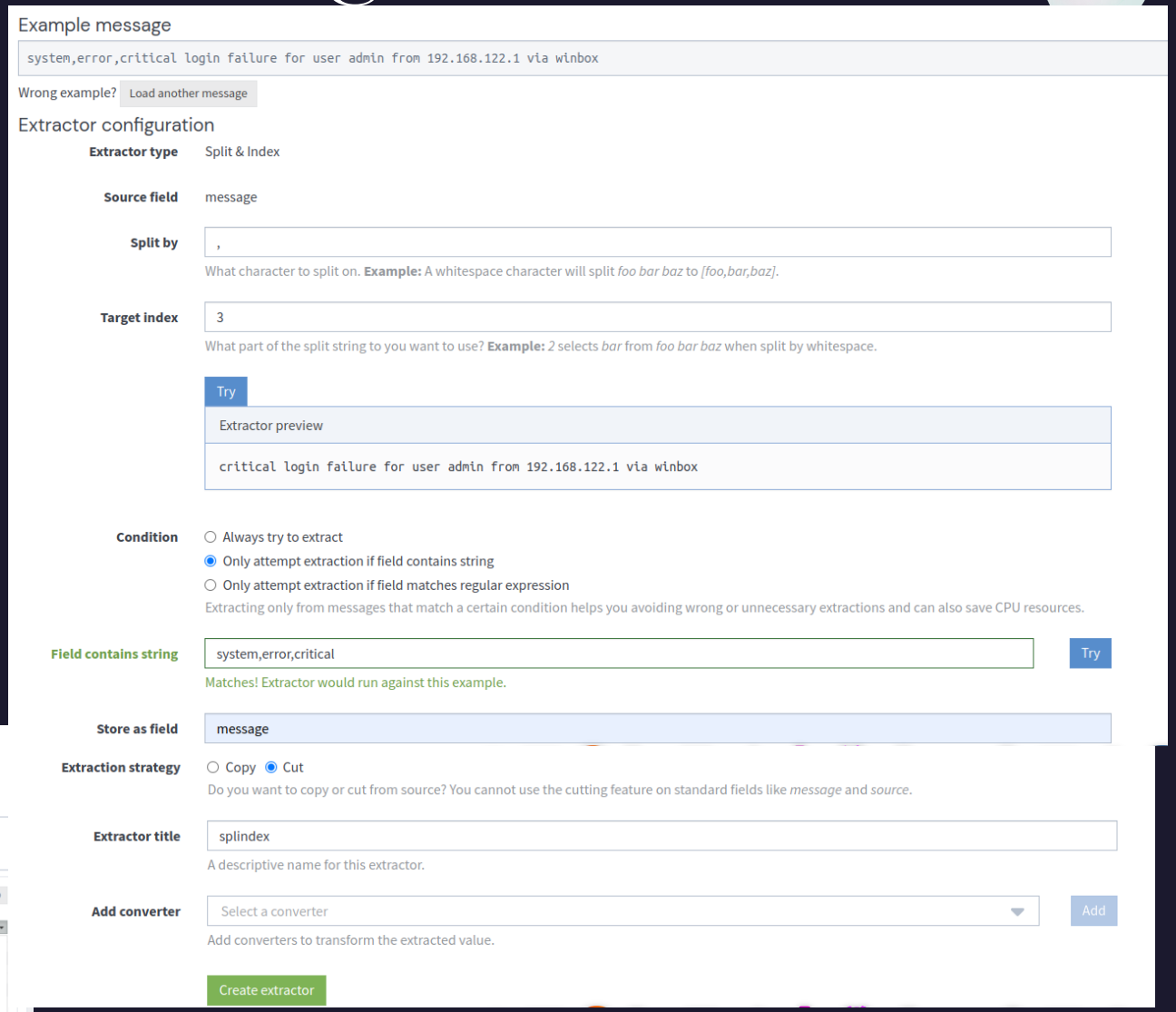




Configurarea colecatorii de log-uri

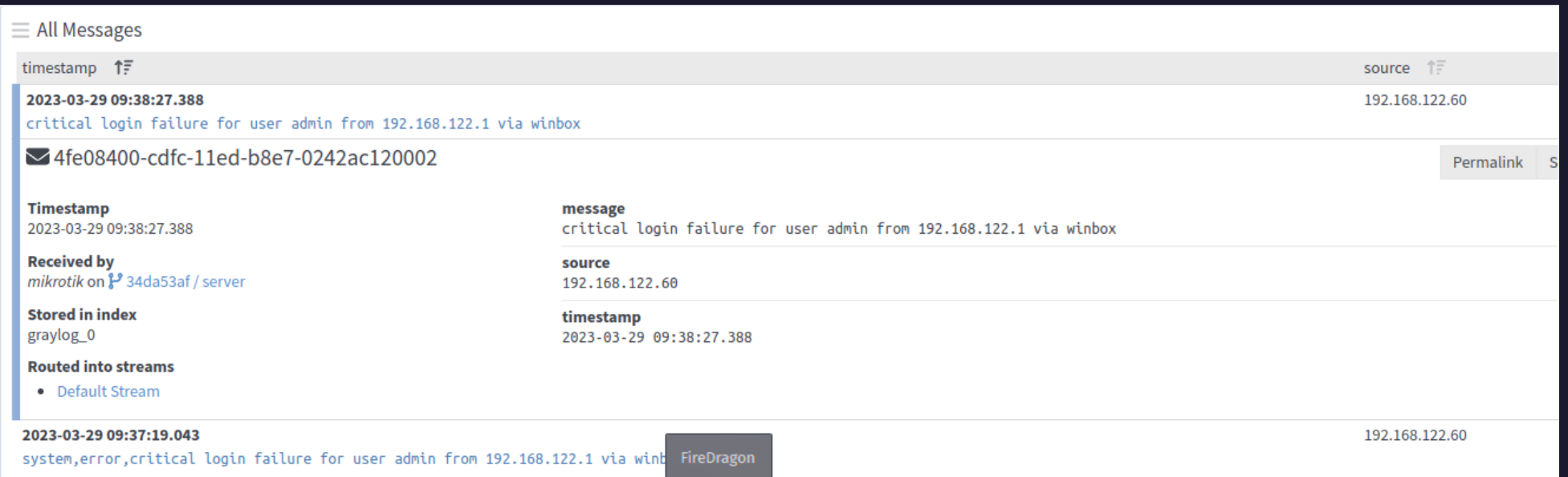
- Ne intoarcem la Inputs si selectam Manage Extractors.
- Facem un extractor nou “Split & Index” pentru a elmina celelate tipuri de eveniment si a pastra doar cel critic.





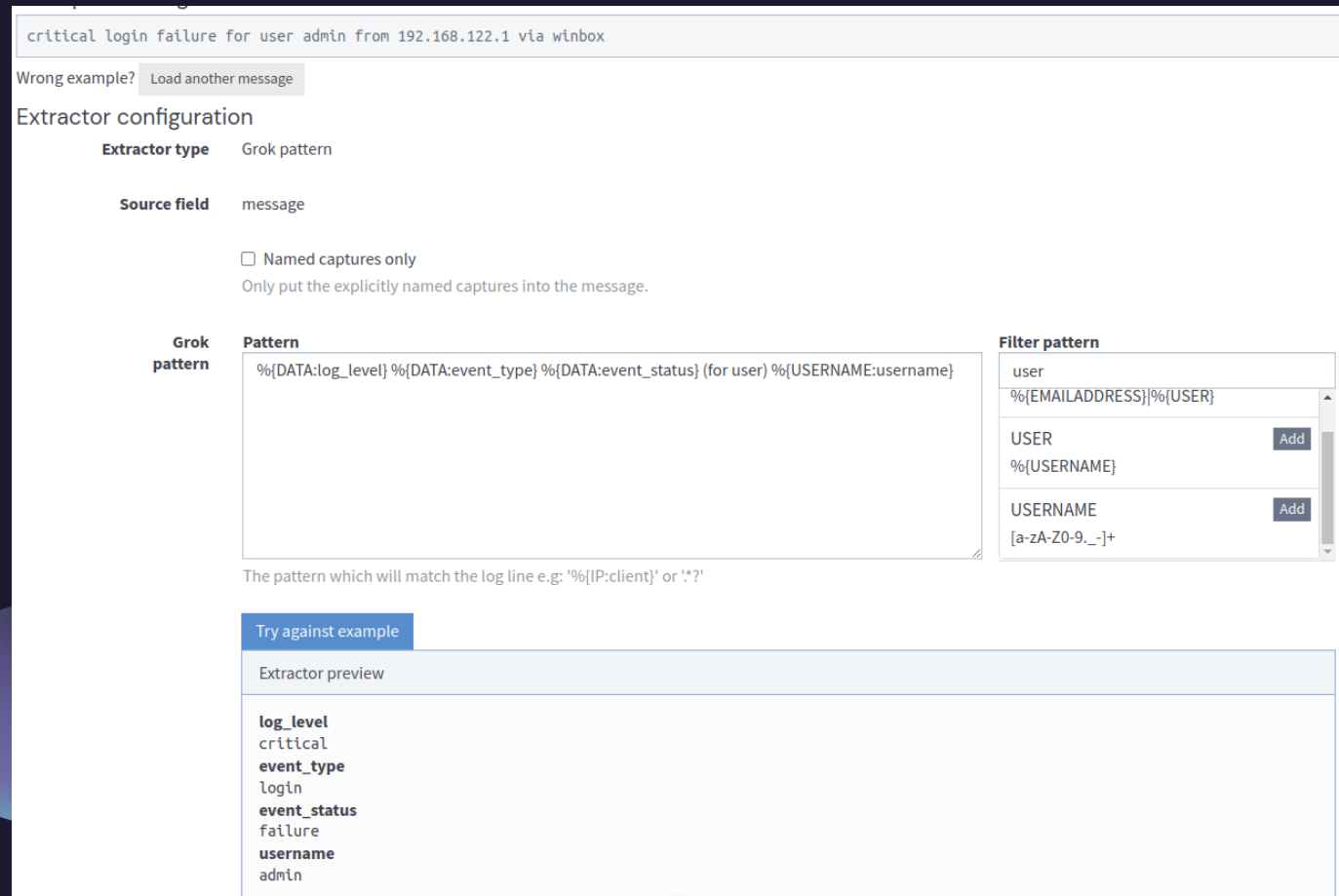
Configurarea colecatorii de log-uri

- Incercam un nou mesaj sa vedem cum arata modificarile si vedem ca mesajul apare modificat dar tot nu este de inteles pentru graylog asa ca vom face inca un extractor de data asta Grok acesta este un extractor bazat pe regular expressions.
- Regula de baza pentru acest tip de filtrare este sa ne gandim ce vrem sa extragem si ce cuvinte sunt statice si vrem sa le folosim ca ancora in mesaj.
- De exemplu incepem cu tipul de eveniment in acest mesaj care poate fi critical,info,etc.



Configurarea colecatorii de log-uri

- Unde avem elemente statice sau pe care vrem sa le eliminam vom folosi parantezele pentru a incapsula continutul exmplu de mai jos avem (for user), atentie la spatii pentru ca lipsa lor sau mai multe spatii vor duce la eroare in extragere.



Configurarea colecatorii de log-uri

- Avem astfel urmatorul pattern pentru a extrage login fails de la logurile mikrotik

Grok pattern

Pattern

%{DATA:log_level} %{DATA:event_type} %{DATA:event_status} (for user) %{USERNAME:username} (from) %{IPV4:ipv4} (via) %{GREEDYDATA:interface}

The pattern which will match the log line e.g: '%{IP:client}' or '.*?'

Filter pattern

gre

GREEDYDATA Add

.*

Try against example

Extractor preview

log_level
critical
event_type
login
event_status
failure
username
admin
ipv4
192.168.122.1
interface
winbox

Configurarea colecatorii de log-uri

- Putem sa testam un alt fail login si sa vedem daca avem mesajul extras corect.
- Si putem obseva ca avem toate field-urile corect extrase, de aici putem sorta face alerte si diferite corelari intre evenimente.
- Am facut un test cu un alt container din retea pe ssh si vedem ca extragerea merge corect.

All Messages

timestamp

2023-03-29 10:11:41.364
critical login failure for user admin from 192.168.122.2 via ssh

f4611b80-ce00-11ed-b8e7-0242ac120002

Timestamp
2023-03-29 10:11:41.364

Received by
mikrotik on 34da53af / server

Stored in index
graylog_0

Routed into streams
- Default Stream

event_status
failure

event_type
login

interface
ssh

ipv4
192.168.122.2

log_level
critical

message
critical login failure for user admin from 192.168.122.2 via ssh

source
192.168.122.60

timestamp
2023-03-29 10:11:41.364

username
admin

All Messages

timestamp

2023-03-29 10:04:33.815
critical login failure for user admin from 192.168.122.1 via winbox

f58d8300-cdff-11ed-b8e7-0242ac120002

Timestamp
2023-03-29 10:04:33.815

Received by
mikrotik on 34da53af / server

Stored in index
graylog_0

Routed into streams
- Default Stream

event_status
failure

event_type
login

interface
winbox

ipv4
192.168.122.1

log_level
critical

message
critical login failure for user admin from 192.168.122.1 via winbox

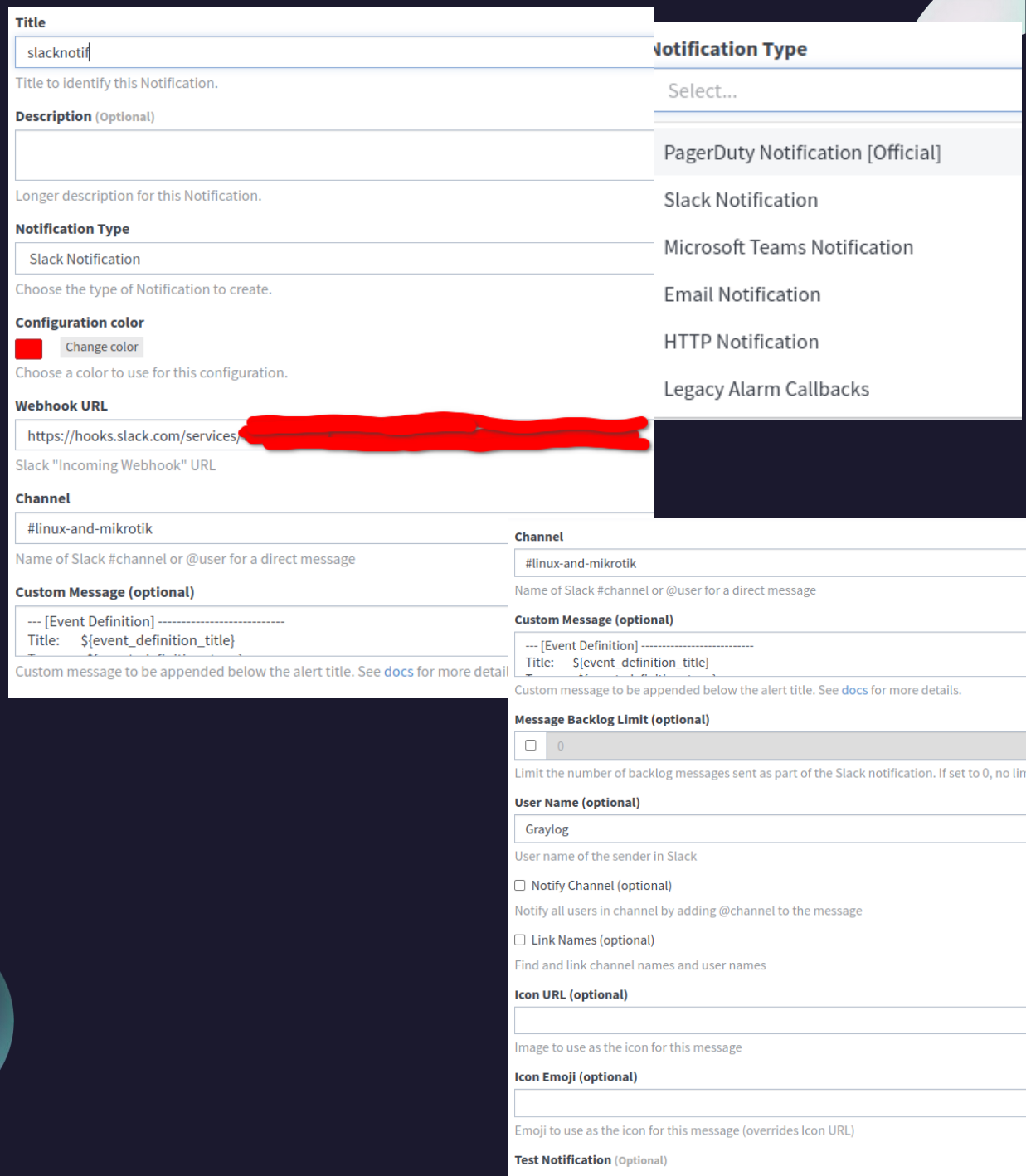
source
192.168.122.60

timestamp
2023-03-29 10:04:33.815

username
admin

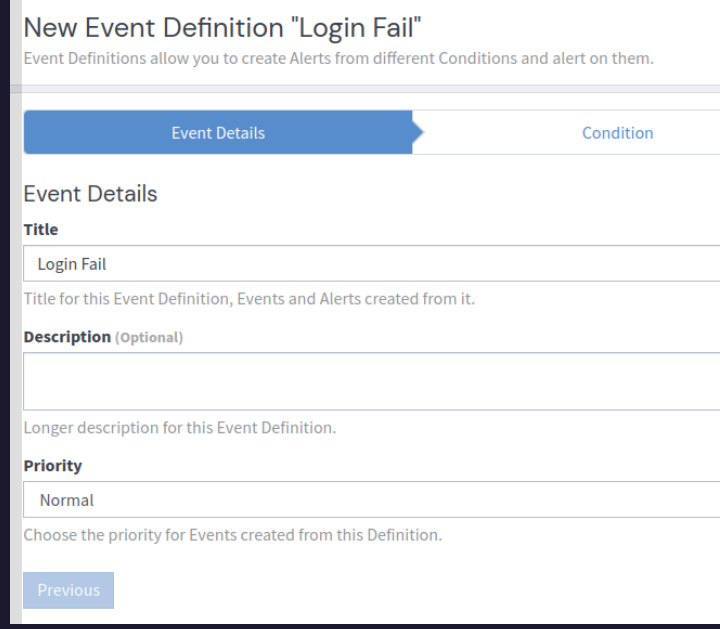
Configurarea alertarii

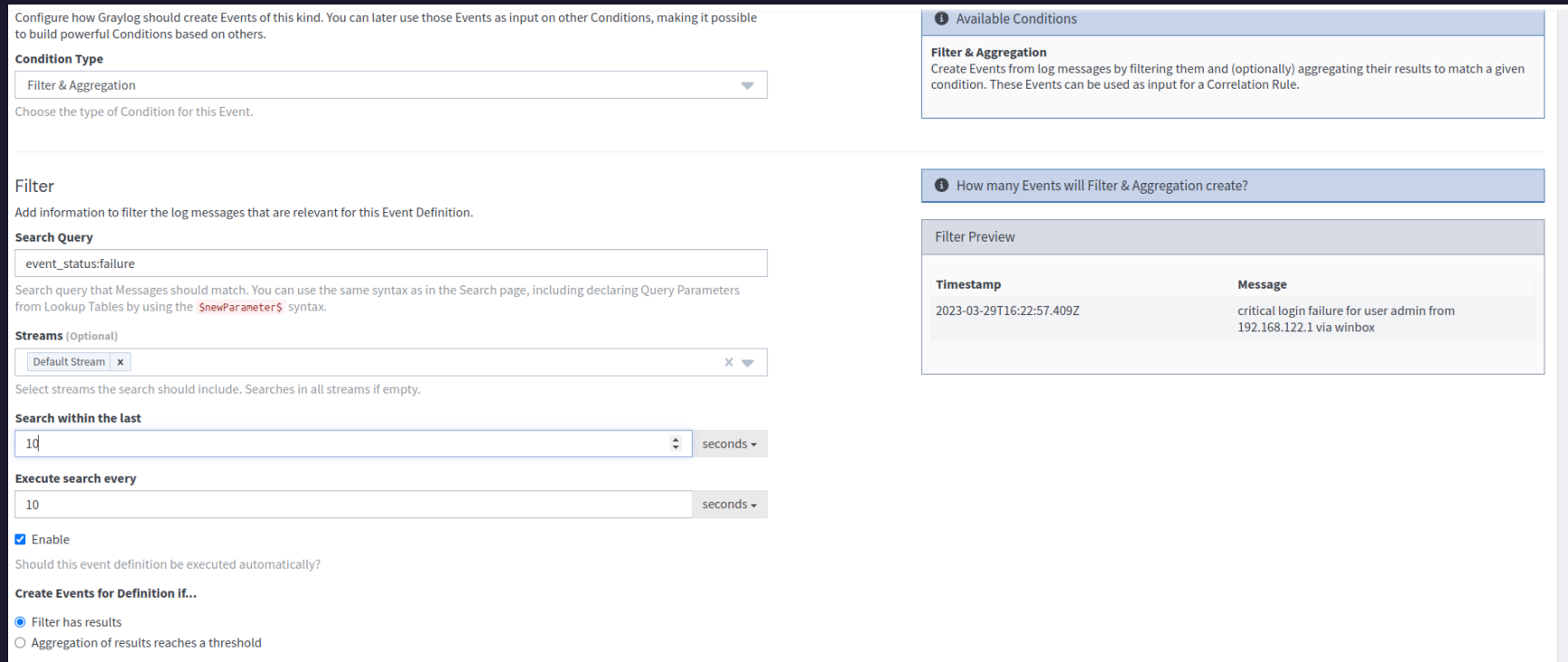
- Graylog suporta mai multe tipuri de alerte, dar pentru acest laborator vom folosi un bot de slack pentru a trimite notificari.
- Mergem in Alerts→Notifications→Create notification iar la Norification Type alegem Slack Notification.
- Url-ul pentru webhook se poate genera din api.slack.com
- Acum ca avem o metoda de a transmite alerta trebuie sa facem conditiile de alertare.



Configurarea alertarii

- Putem sa facem defintia megand la Alerts→Event Definitions→Create event definition si avem de completat cateva campuri.
- In Search Query punem un query pe care il facem in sectiunea se search.
- Setam intervalul de timp
- pentru care vrem sa scanam
- evenimentele.





Configurarea alertarii

- In sectiunea fields vom adauga ce campuri vrem sa adaugam in mesaj.
- Numele este cel care va fi afisat in alerta si Set Value From setam campul din mesaj pe care sa il populam de forma ${source.<nume_camp>}.
- La notificari adaugam notificare sau notificarile facute mai devreme.

Event Details | Filter & Aggregation | Fields

New Custom Field

Name

Attacker IP

Name for this Field.

Use Field as Event Key

1

Indicates if this Field should be a Key and its order.

Field Data Type

String

Set Value From

Template

Select a source for the value of this Field.

Template

${source.ipv4}

Type a literal text to set to this Field or use JMTE syntax to add a dynamic Value.

Require all template values to be set

Check this option to validate that all variables used in the Template have values.

Field Name	Is Key?	Value Source	Data Type	Configuration	Actions
Attacker IP	No	Template	string	template: *"${source.ipv4}"*	Remove Field Edit
Event Type	No	Template	string	template: *"${source.event_type}"*	Remove Field Edit
Username	No	Template	string	template: *"${source.username}"*	Remove Field Edit

Event Details | Filter & Aggregation | Fields | Notifications

Notifications (optional) Manage Notifications

Is this Event important enough that requires your attention? Make it an Alert by adding Notifications to it.

Notification	Type	Actions
slacknotif	Slack Notification	Remove from Event

Add Notification

Notification Settings

Grace Period

0 seconds

Graylog sends Notifications for Alerts every time they occur. Set a Grace Period to control how long Graylog should wait before sending Notifications again. Note that Events with keys will have a Grace Period for each different key value.

Message Backlog

50

Number of messages to be included in Notifications.

Configurarea alertarii

- Putem verifica mesajele in Slack dupa ce incercam un failed login.