

# 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_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.

## ADD A NEW NODE

Template

Linux

Number of nodes to add

1

Image

linux-docker

Name/prefix

Linux

Icon

Server.png

UUID

CPU Limit

☐

CPU

2

RAM (MB)

4096

Ethernets

1

First Eth MAC Address

QEMU Version

tpl(default 2.4.0)

QEMU Arch

tpl(x86\_64)

QEMU Nic

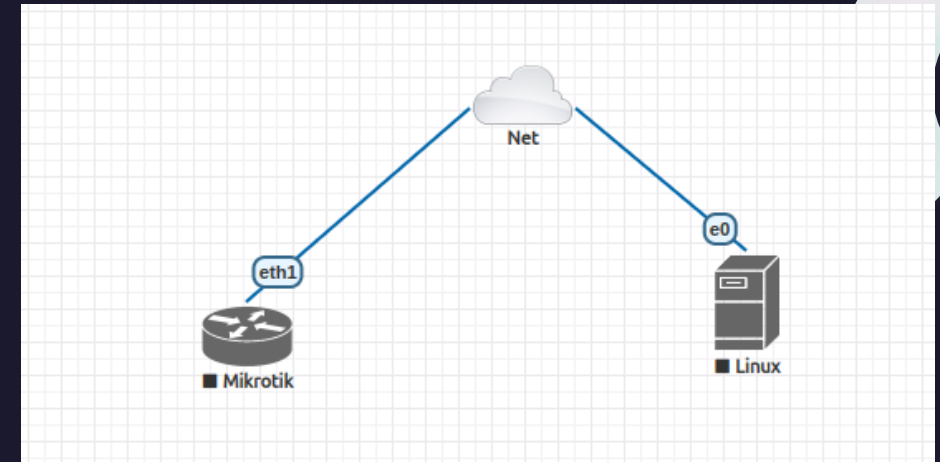
tpl(virtio-net-pci)

QEMU custom options

-machine type=pc,accel=kvm -vga std -usbdevice tablet -boot order=cd -cpu host

# Setup-ul initial

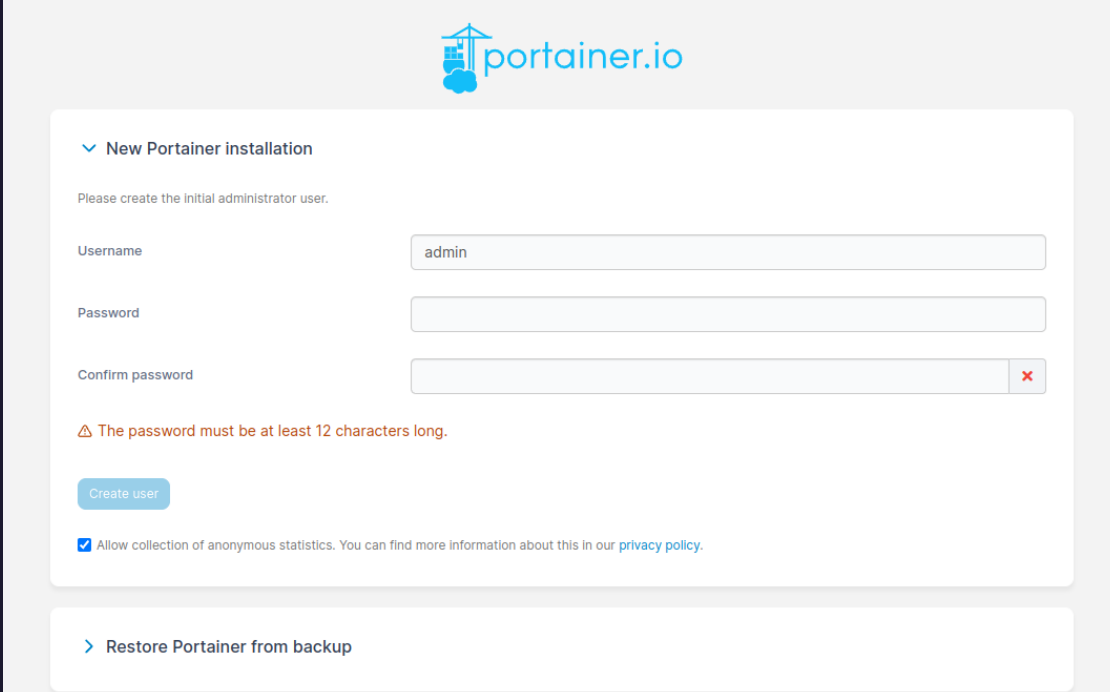
- Se poate instala si un server virtual separat si configurat sau orice alta metoda care duce la instalarea acestui server, calea aleasa de mine este cea mai usoara varianta de instalare in laboratorul virtual.
- Punem si un router Mikrotik legeat la internet impreuna cu serverul nostru si pornim serverul.
- 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`



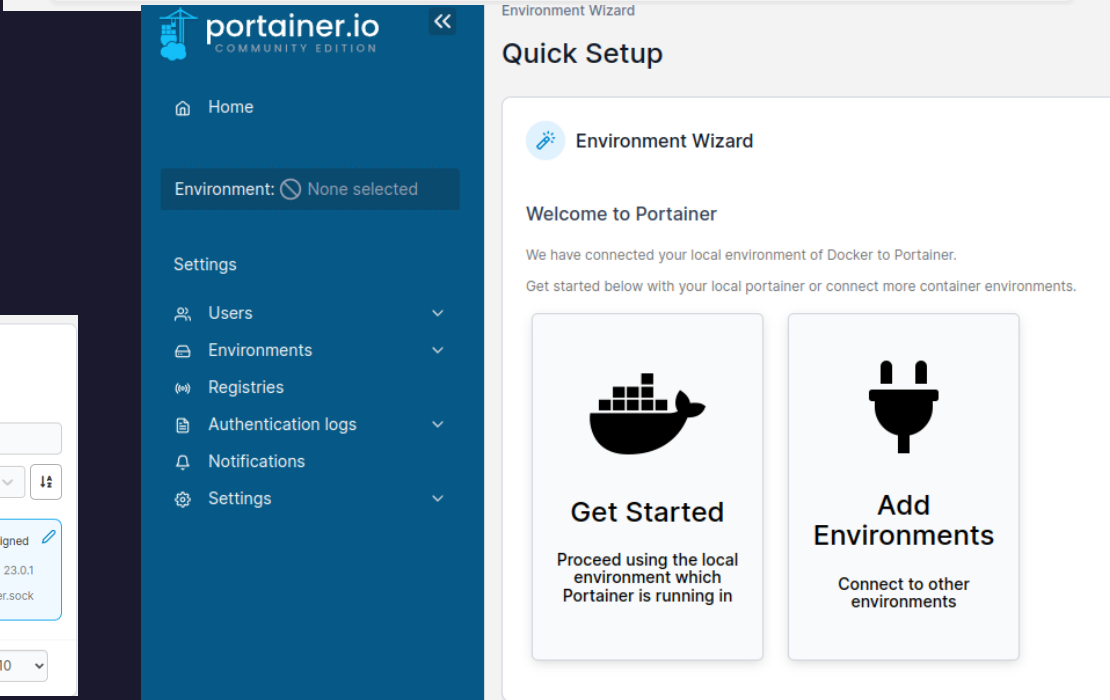
```
[root@docker ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft 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: veth94ed7f2eif4: <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

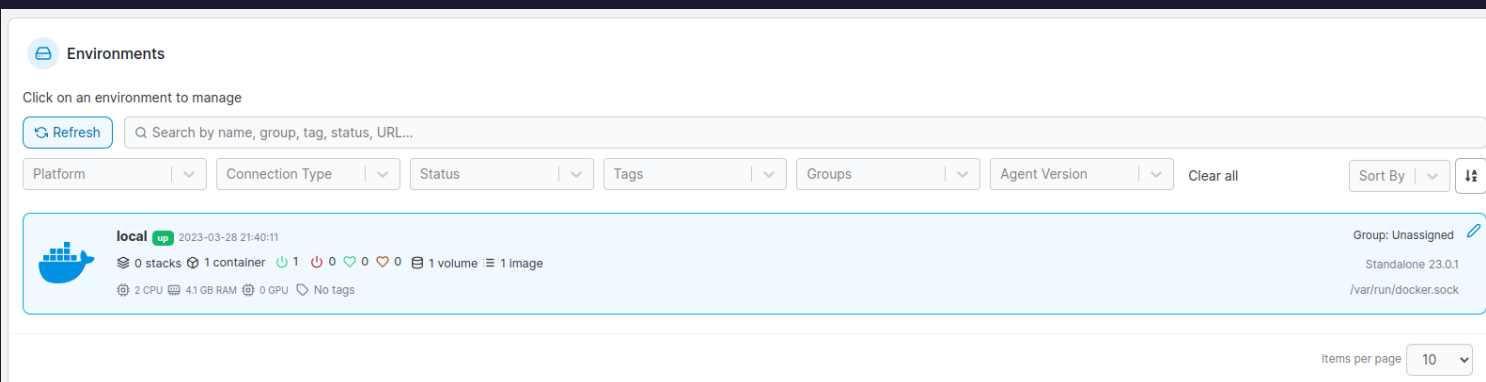
- Acum ca am ajuns la interfata de administrare ne setam parola.
- Apoi dam pe Get Started si vedem instanta locala preconfigurata.



The image shows the 'New Portainer installation' form. It includes fields for Username (admin), Password, and Confirm password. A message states: 'The password must be at least 12 characters long.' There is a 'Create user' button and a checkbox for 'Allow collection of anonymous statistics'.



The image shows the 'Quick Setup' screen of the Portainer Environment Wizard. It includes a sidebar with navigation links: Home, Environment (None selected), Settings, Users, Environments, Registries, Authentication logs, Notifications, and Settings. The main content area has a 'Welcome to Portainer' message and two buttons: 'Get Started' and 'Add Environments'.



The image shows the 'Environments' section of the Portainer interface. It includes a search bar, filters for Platform, Connection Type, Status, Tags, Groups, and Agent Version, and a table of environments. The table shows a single environment named 'local' with status 'up', created on 2023-03-28 at 21:40:11, and details: 0 stacks, 1 container, 1 volume, 1 image, 2 CPU, 41 GB RAM, 0 GPU, No tags. The environment is assigned to the 'Unassigned' group and is running on 'Standalone 23.0.1' with the socket path '/var/run/docker.sock'.

# 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.

The screenshot displays the Portainer.io Community Edition web interface. On the left is a dark blue sidebar with navigation links: Home, local (selected), Dashboard, App Templates, Stacks, Containers, Images, Networks, and Volumes. The main content area is titled 'Stacks' and 'Stacks list'. It features a search bar, a 'Remove' button, and an 'Add stack' button. Below these is a table with columns: Name, Type, Control, Created, and Ownership. The table is currently empty, showing 'No stack available.' at the bottom. The top right corner shows a user profile for 'admin'.

portainer.io  
COMMUNITY EDITION

Stacks

Stacks list

Search for a stack...

Remove + Add stack

Name ↓↑ Filter ▼	Type ↓↑	Control	Created ↓↑	Ownership ↓↑
No stack available.				

Items per page 10 ▼

# Instalarea Graylog

- Trebuie sa modificam in principiu 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:

"7dgPW4OOVd8lSaajcQVY8hnESsXxd5Gj8omkmjWtp1N5BogTXr1Yy3HfGOqVIR2F0xOvcV8ppMm7pUnkJl9ElmbMI7XhJO4w"

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:

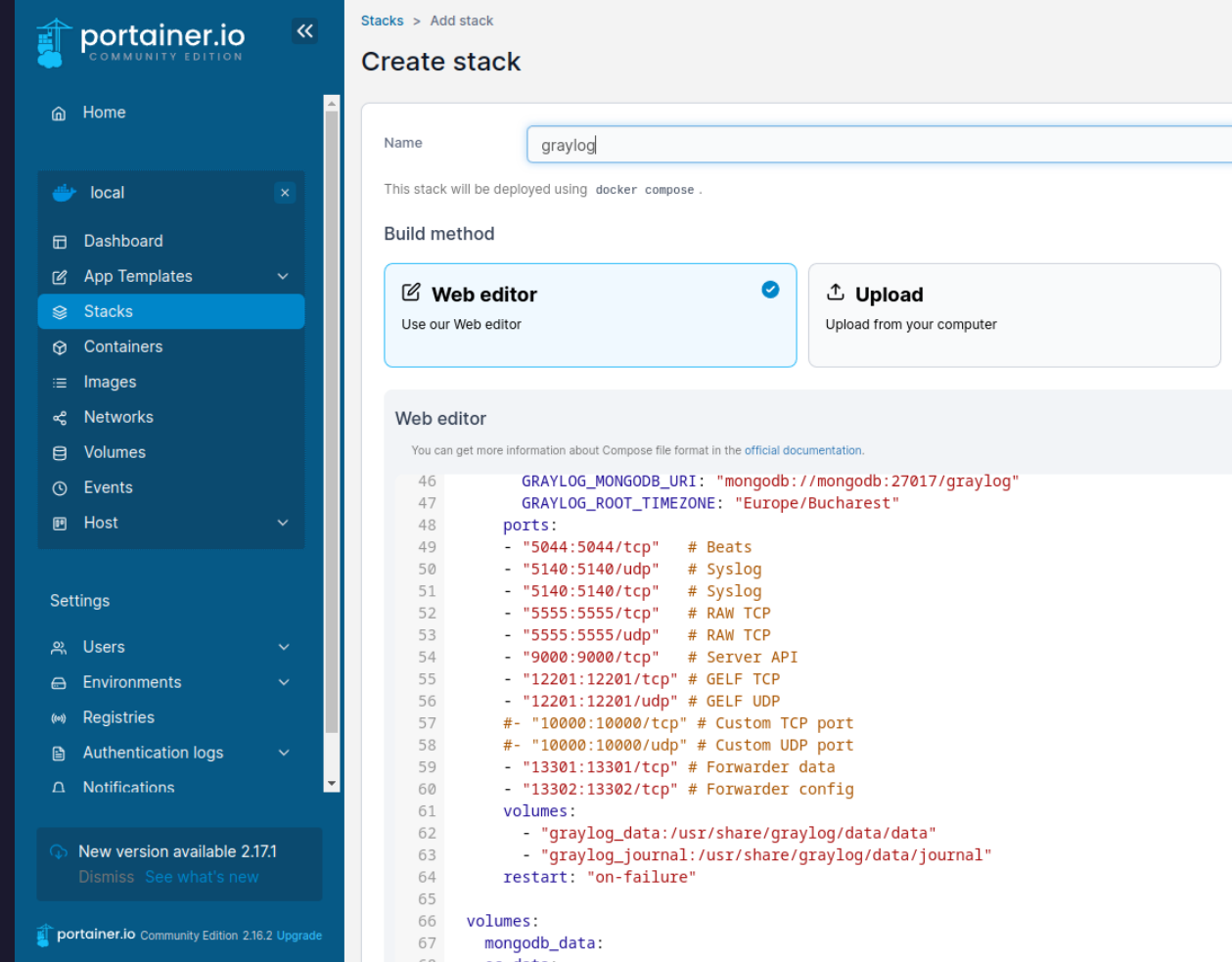
os\_data:

opensearch\_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.



portainer.io COMMUNITY EDITION

Stacks > Add stack

## Create stack

Name:

This stack will be deployed using `docker compose`.

Build method

**Web editor** (selected) Use our Web editor

**Upload** Upload from your computer

Web editor

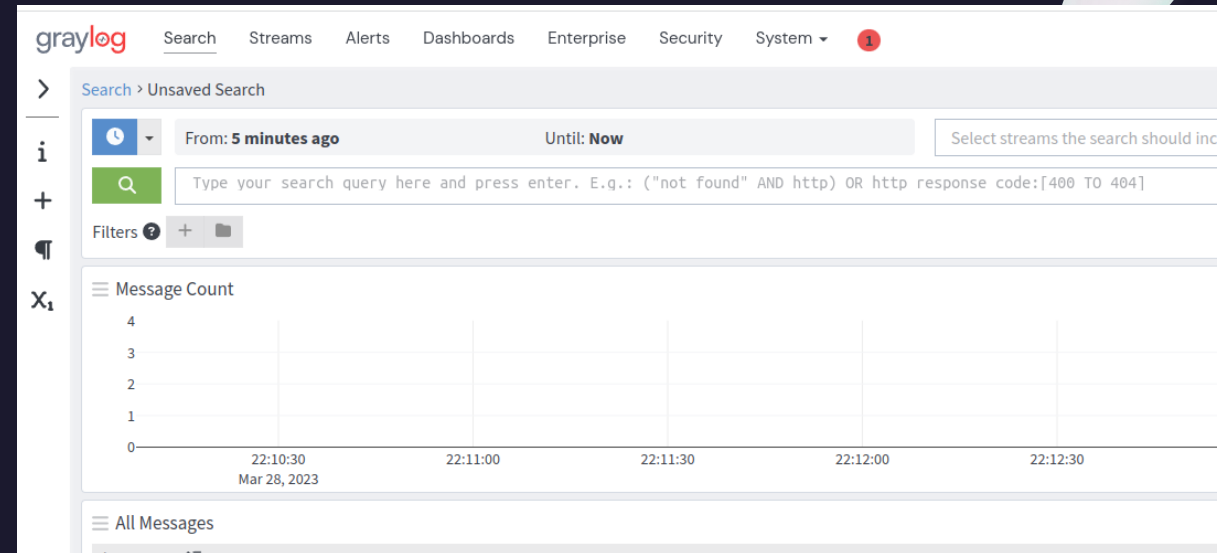
You can get more information about Compose file format in the [official documentation](#).

```
46 GRAYLOG_MONGODB_URI: "mongodb://mongodb:27017/graylog"
47 GRAYLOG_ROOT_TIMEZONE: "Europe/Bucharest"
48 ports:
49   - "5044:5044/tcp" # Beats
50   - "5140:5140/udp" # Syslog
51   - "5140:5140/tcp" # Syslog
52   - "5555:5555/tcp" # RAW TCP
53   - "5555:5555/udp" # RAW TCP
54   - "9000:9000/tcp" # Server API
55   - "12201:12201/tcp" # GELF TCP
56   - "12201:12201/udp" # GELF UDP
57   #- "10000:10000/tcp" # Custom TCP port
58   #- "10000:10000/udp" # Custom UDP port
59   - "13301:13301/tcp" # Forwarder data
60   - "13302:13302/tcp" # Forwarder config
61 volumes:
62   - "graylog_data:/usr/share/graylog/data/data"
63   - "graylog_journal:/usr/share/graylog/data/journal"
64 restart: "on-failure"
65
66 volumes:
67   mongodb_data:
68     data:
```

Containers									
Q Search...									
▶ Start ◻ Stop ⌛ Kill ↺ Restart ⏸ Pause ▶ Resume 🗑 Remove ⌵									
☐ Name ↓↑	State ↓↑ Filter	Quick Actions	Stack ↓↑	Image ↓↑	Created ↓↑	IP Address ↓↑	GPUs	Published Ports	
☐ graylog-graylog-1	starting	📄 ⓘ ⌵ ⌶ 🔗	graylog	graylog/graylog:5.0	2023-03-28 22:00:48	172.18.0.4	none	🔗12201:12201 🔗13302:13302 🔗5140:5140 🔗5555:5555 🔗9000:9000 🔗13301:13301	
☐ graylog-mongodb-1	running	📄 ⓘ ⌵ ⌶ 🔗	graylog	mongo:5.0	2023-03-28 22:00:48	172.18.0.2	none	-	
☐ graylog-opensearch-1	running	📄 ⓘ ⌵ ⌶ 🔗	graylog	opensearchproject/opensearch:2.4.0	2023-03-28 22:00:48	172.18.0.3	none	-	

# Instalarea Graylog

- In logurile de initializare ale containerului graylog putem vedea ca a pornit cu succes 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 19:01:46,244 INFO : org.graylog.plugins.pipelineprocessor.periodical.LegacyDefaultStreamMigration - Legacy default stream
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 colecătorii 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.
- Selecăm un port care este mapat din container (ex: 5555).
- Acest input acționează ca un listener și primește de la un client mesaje

**Inputs**  
Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

Select input ▲ Launch new input Find more inputs

Reset

**Launch new Raw/Plaintext UDP input**

☐ Global  
Should this input start on all nodes

**Node**  
34da53af / server

On which node should this input start

**Title**  
mikrotik

Select a name of your new input that describes it.

**Bind address**  
0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

**Port**  
5555

Port to listen on.

**Receive Buffer Size (optional)**  
262144

The size in bytes of the recvBufferSize for network connections to this input.

**No. of worker threads (optional)**  
2

Number of worker threads processing network connections for this input.

**Override source (optional)**

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

**Encoding (optional)**  
UTF-8

Default encoding is UTF-8. Set this to a standard charset name if you want override the default.

## Global inputs 0 configured

There are no global inputs.

## Local inputs 1 configured

**mikrotik** Raw/Plaintext UDP RUNNING  
On node 34da53af / server

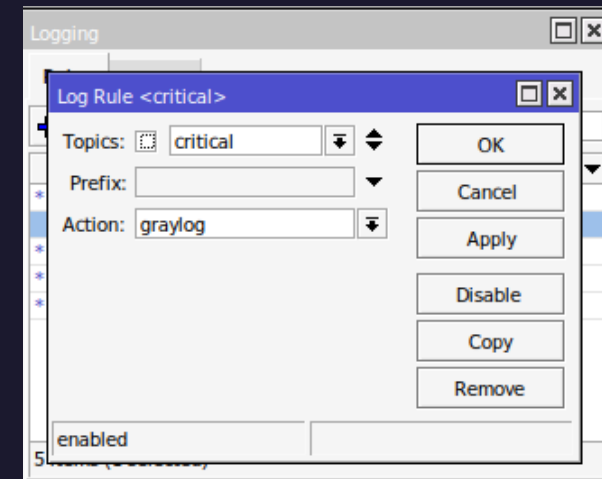
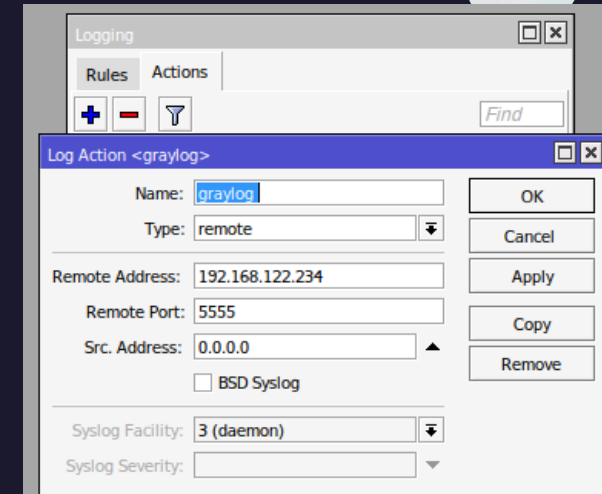
bind\_address: 0.0.0.0  
charset\_name: UTF-8  
number\_worker\_threads: 2  
override\_source: <empty>  
port: 5555  
recv\_buffer\_size: 262144

Show received messages Manage extractors Stop input More actions

**Throughput / Metrics**  
1 minute average rate: 0 msg/s  
Network IO: ▼0B ▲0B (total: ▼0B ▲0B)  
Empty messages discarded: 0

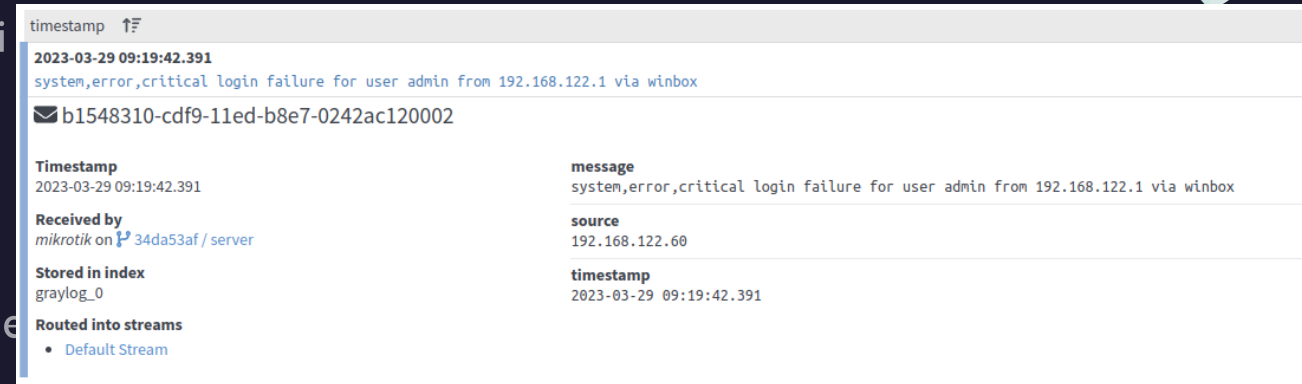
# Configurarea colecatorii de log-uri

- 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.

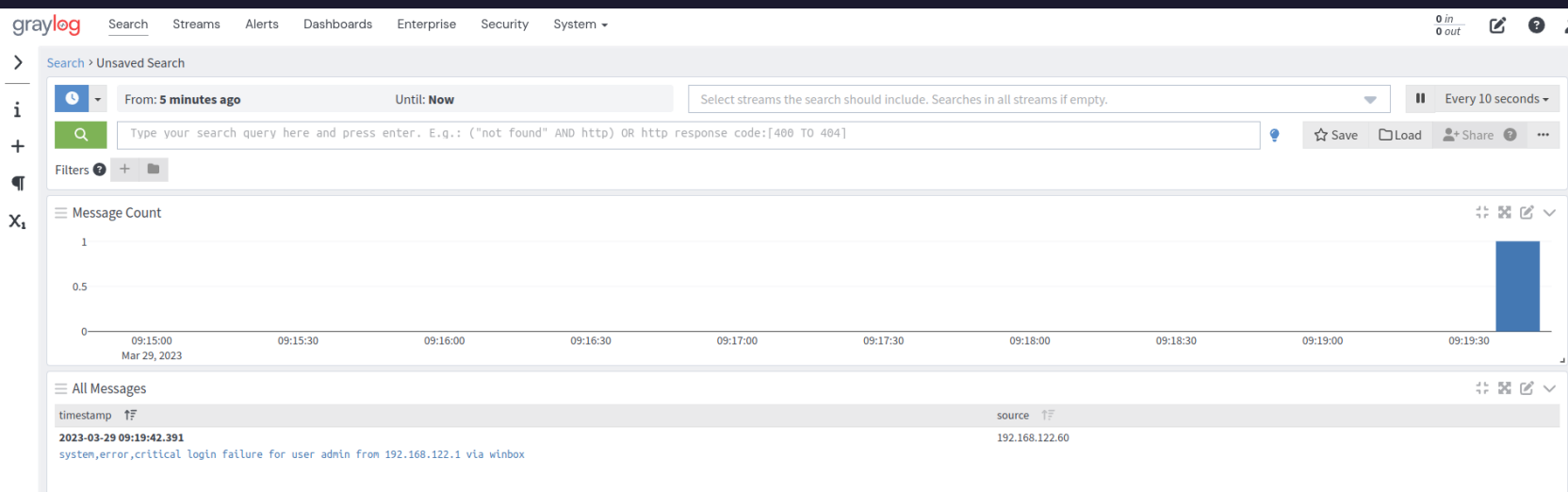


timestamp ↑

**2023-03-29 09:19:42.391**  
system,error,critical login failure for user admin from 192.168.122.1 via winbox

✉ b1548310-cdf9-11ed-b8e7-0242ac120002

<b>Timestamp</b> 2023-03-29 09:19:42.391	<b>message</b> system,error,critical login failure for user admin from 192.168.122.1 via winbox
<b>Received by</b> mikrotik on 34da53af / server	<b>source</b> 192.168.122.60
<b>Stored in index</b> graylog_0	<b>timestamp</b> 2023-03-29 09:19:42.391
<b>Routed into streams</b> <ul style="list-style-type: none"><li>Default Stream</li></ul>	



# Configurarea colecatorii de log-uri

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

Add extractor

Start by loading a message to have an example to work on. You can decide whether to load a recent message received by this input, or manually select a message giving its ID.

Create extractor

Recent Message

Message ID

Click on "Load Message" to load the most recent message received by this input within the last hour.

mikrotik (org.graylog2.inputs.raw.udp.RawUDPInput)

Load Message

b1548310-cdf9-11ed-b9e7-0242ac120002

Permalink

Copy ID

Select extractor type ▾

Copy input

Grok pattern

JSON

Regular expression

Replace with regular expression

Split & Index

Substring

Lookup Table

Timestamp

2023-03-29 09:19:42

Stored in index

graylog\_0

Routed into streams

Default Stream

message

system,error,critical login failure for user admin from 192.168.122.1 via winbox

source

192.168.122.60

timestamp

2023-03-29T06:19:42.391Z

Configured extractors

This input has no configured extractors.

Example message

system,error,critical login failure for user admin from 192.168.122.1 via winbox

Wrong example?

Load another message

Extractor configuration

Extractor type

Split & Index

Source field

message

Split by

,

What character to split on. **Example:** A whitespace character will split *foo bar baz* to *[foo,bar,baz]*.

Target index

3

What part of the split string to you want to use? **Example:** 2 selects *bar* from *foo bar baz* when split by whitespace.

Try

Extractor preview

critical login failure for user admin from 192.168.122.1 via winbox

Condition

☐ Always try to extract

☒ Only attempt extraction if field contains string

☐ Only attempt extraction if field matches regular expression

Extracting only from messages that match a certain condition helps you avoiding wrong or unnecessary extractions and can also save CPU resources.

Field contains string

system,error,critical

Matches! Extractor would run against this example.

Try

Store as field

message

Extraction strategy

☐ Copy

☒ Cut

Do you want to copy or cut from source? You cannot use the cutting feature on standard fields like *message* and *source*.

Extractor title

splindex

A descriptive name for this extractor.

Add converter

Select a converter ▾

Add

Add converters to transform the extracted value.

Create extractor

# 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.

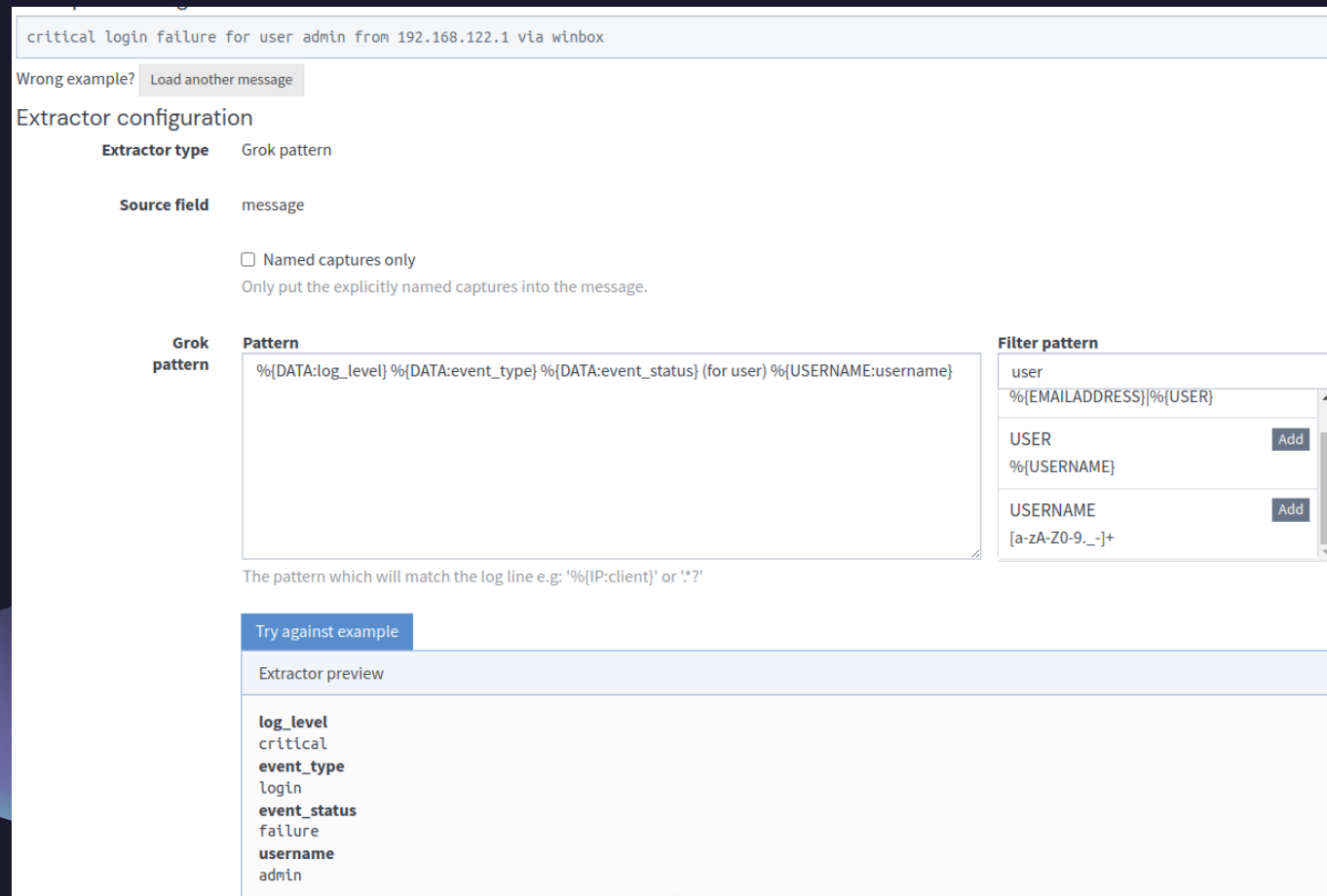
≡ All Messages

timestamp ↑	source ↑
<b>2023-03-29 09:38:27.388</b> critical login failure for user admin from 192.168.122.1 via winbox	192.168.122.60
✉ 4fe08400-cdfc-11ed-b8e7-0242ac120002 <span>Permalink</span> <span>S</span>	
<b>Timestamp</b> 2023-03-29 09:38:27.388	<b>message</b> critical login failure for user admin from 192.168.122.1 via winbox
<b>Received by</b> mikrotik on <a href="#">34da53af / server</a>	<b>source</b> 192.168.122.60
<b>Stored in index</b> graylog_0	<b>timestamp</b> 2023-03-29 09:38:27.388
<b>Routed into streams</b> <ul style="list-style-type: none"><li>• <a href="#">Default Stream</a></li></ul>	
<b>2023-03-29 09:37:19.043</b> system,error,critical login failure for user admin from 192.168.122.1 via winb	192.168.122.60

FireDragon

# 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.



The screenshot shows the Logstash configuration page for a Grok pattern. At the top, a sample log message is displayed: "critical login failure for user admin from 192.168.122.1 via winbox". Below this, the "Extractor configuration" section is visible. The "Extractor type" is set to "Grok pattern" and the "Source field" is "message". There is an unchecked checkbox for "Named captures only" with a note: "Only put the explicitly named captures into the message." The "Grok pattern" section contains a text area with the pattern: "%{DATA:log\_level} %{DATA:event\_type} %{DATA:event\_status} (for user) %{USERNAME:username}". To the right, the "Filter pattern" section shows a list of patterns: "user" (with a sub-pattern "%{EMAILADDRESS}}%{USER}"), "USER" (with a sub-pattern "%{USERNAME}"), and "USERNAME" (with a sub-pattern "[a-zA-Z0-9.\_-]+"). Each has an "Add" button. Below the pattern configuration, there is a "Try against example" button and an "Extractor preview" section. The preview shows the following extracted fields: log\_level (critical), event\_type (login), event\_status (failure), and username (admin).

critical login failure for user admin from 192.168.122.1 via winbox

Wrong example? [Load another message](#)

### Extractor configuration

**Extractor type** Grok pattern

**Source field** message

☐ Named captures only  
Only put the explicitly named captures into the message.

**Grok pattern**

**Pattern**

%{DATA:log\_level} %{DATA:event\_type} %{DATA:event\_status} (for user) %{USERNAME:username}

**Filter pattern**

user  
%{EMAILADDRESS}}%{USER}

USER  
%{USERNAME}

USERNAME  
[a-zA-Z0-9.\_-]+

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

[Try against example](#)

Extractor preview

**log\_level**  
critical  
**event\_type**  
login  
**event\_status**  
failure  
**username**  
admin



# Configurarea colecătorii 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}

**Filter pattern**  
gre  
GREEDYDATA  
.\*  
[Add](#)

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

[Try against example](#)

**Extractor preview**  
**log\_level**  
critical  
**event\_type**  
login  
**event\_status**  
failure  
**username**  
admin  
**ipv4**  
192.168.122.1  
**interface**  
winbox

# Configurarea colectorii 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	event_status failure
Received by mikrotik on 34da53af / server	event_type login
Stored in index graylog_0	interface ssh
Routed into streams • Default Stream	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	event_status failure
Received by mikrotik on 34da53af / server	event_type login
Stored in index graylog_0	interface winbox
Routed into streams • Default Stream	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 Notification 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.

<b>Title</b>	<b>Notification Type</b>
<input type="text" value="slacknotifi"/>	Select...
<small>Title to identify this Notification.</small>	
<b>Description (Optional)</b>	PagerDuty Notification [Official]
<input type="text"/>	Slack Notification
<small>Longer description for this Notification.</small>	Microsoft Teams Notification
<b>Notification Type</b>	Email Notification
<input type="text" value="Slack Notification"/>	HTTP Notification
<small>Choose the type of Notification to create.</small>	Legacy Alarm Callbacks
<b>Configuration color</b>	
<input type="color" value="red"/> <input type="button" value="Change color"/>	
<small>Choose a color to use for this configuration.</small>	
<b>Webhook URL</b>	
<input type="text" value="https://hooks.slack.com/services/..."/>	
<small>Slack "Incoming Webhook" URL</small>	
<b>Channel</b>	
<input type="text" value="#linux-and-mikrotik"/>	<b>Channel</b>
<small>Name of Slack #channel or @user for a direct message</small>	<input type="text" value="#linux-and-mikrotik"/>
<small>Name of Slack #channel or @user for a direct message</small>	
<b>Custom Message (optional)</b>	<b>Custom Message (optional)</b>
<input type="text" value="--- [Event Definition] ---\nTitle: \${event_definition_title}"/>	<input type="text" value="--- [Event Definition] ---\nTitle: \${event_definition_title}"/>
<small>Custom message to be appended below the alert title. See <a href="#">docs</a> for more details.</small>	<small>Custom message to be appended below the alert title. See <a href="#">docs</a> for more details.</small>
	<b>Message Backlog Limit (optional)</b>
	<input type="checkbox"/> 0
	<small>Limit the number of backlog messages sent as part of the Slack notification. If set to 0, no limit.</small>
	<b>User Name (optional)</b>
	<input type="text" value="Graylog"/>
	<small>User name of the sender in Slack</small>
	<input type="checkbox"/> <b>Notify Channel (optional)</b>
	<small>Notify all users in channel by adding @channel to the message</small>
	<input type="checkbox"/> <b>Link Names (optional)</b>
	<small>Find and link channel names and user names</small>
	<b>Icon URL (optional)</b>
	<input type="text"/>
	<small>Image to use as the icon for this message</small>
	<b>Icon Emoji (optional)</b>
	<input type="text"/>
	<small>Emoji to use as the icon for this message (overrides Icon URL)</small>
	<b>Test Notification (Optional)</b>

# 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.



Configure how Graylog should create Events of this kind. You can later use those Events as input on other Conditions, making it possible to build powerful Conditions based on others.

## Condition Type

Filter & Aggregation

Choose the type of Condition for this Event.

## Filter

Add information to filter the log messages that are relevant for this Event Definition.

### Search Query

event\_status:failure

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

### Streams (Optional)

Default Stream

Select streams the search should include. Searches in all streams if empty.

### Search within the last

1d

seconds

### Execute search every

10

seconds

☒ Enable

Should this event definition be executed automatically?

### Create Events for Definition if...

☒ Filter has results

☐ Aggregation of results reaches a threshold

## New Event Definition "Login Fail"

Event Definitions allow you to create Alerts from different Conditions and alert on them.

Event Details

Condition

## Event Details

### Title

Login Fail

Title for this Event Definition, Events and Alerts created from it.

### Description (Optional)

Longer description for this Event Definition.

### Priority

Normal

Choose the priority for Events created from this Definition.

Previous

## Available Conditions

### Filter & Aggregation

Create Events from log messages by filtering them and (optionally) aggregating their results to match a given condition. These Events can be used as input for a Correlation Rule.

## How many Events will Filter & Aggregation create?

## Filter Preview

### Timestamp

2023-03-29T16:22:57.409Z

### Message

critical login failure for user admin from 192.168.122.1 via winbox

# 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}"	<div>Remove FieldEdit</div>
Event Type	No	Template	string	template: "\${source.event_type}"	<div>Remove FieldEdit</div>
Username	No	Template	string	template: "\${source.username}"	<div>Remove FieldEdit</div>

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	<div>Remove from Event</div>

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.



**Graylog** APP 7:34 PM

**Alert Login Fail** triggered:

Custom Message:

--- [Event Definition] -----

Title: Login Fail

Type: aggregation-v1

--- [Event] -----

Timestamp: 2023-03-29T16:34:42.664Z

Message: Login Fail

Source: server

Priority: 2

Alert: true

Timestamp Processing: 2023-03-29T16:34:42.664Z

Event Fields:

Event\_Type: login

Attacker\_IP: 192.168.122.1

Username: admin

[Show less](#)