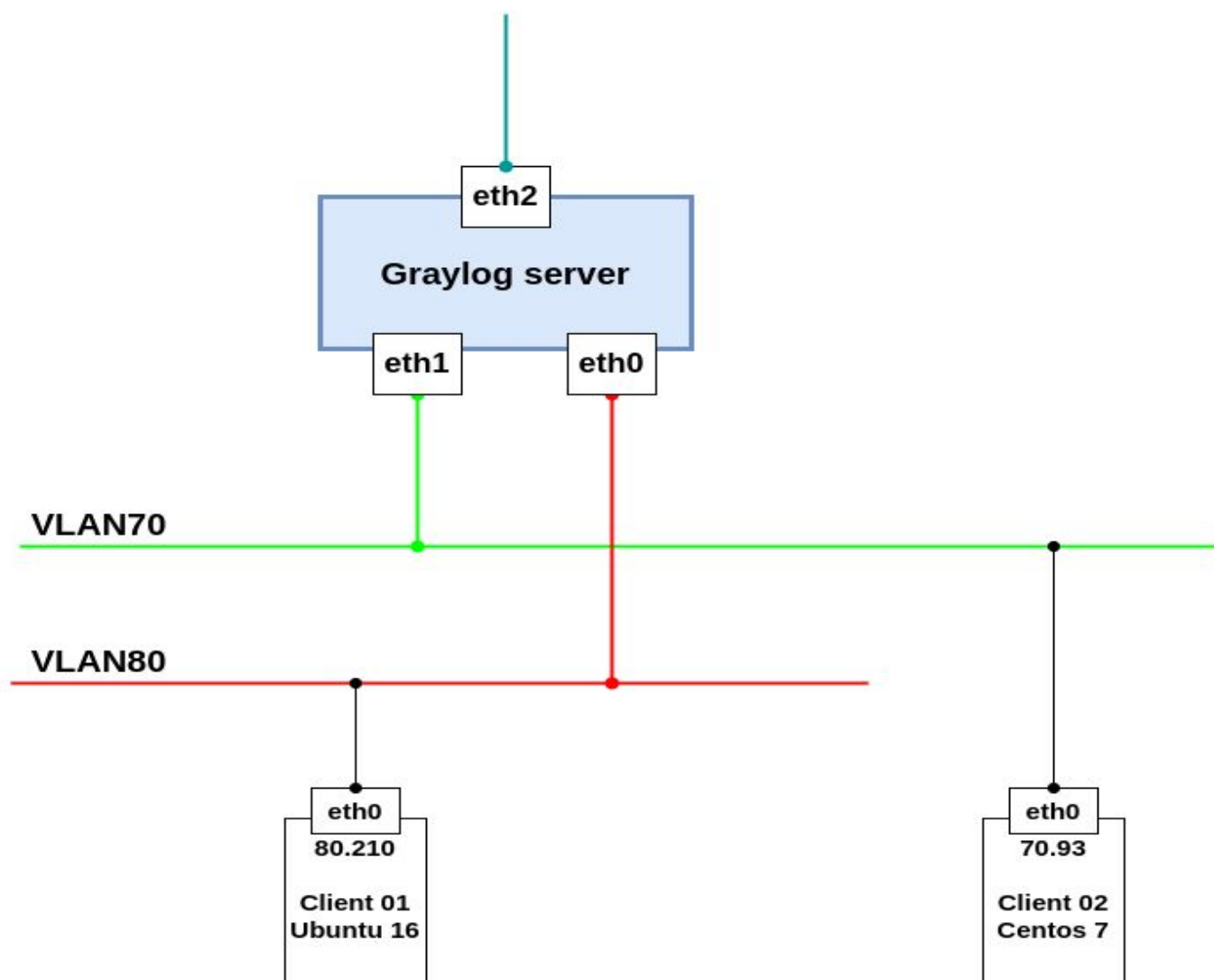


1. Mô hình triển khai

1.1 Mô hình IP planning

IP Planning					
Name	OS	Interface	IP	Cấu hình phần cứng	Ghi chú
Graylog Server	Centos 7	eth0	192.168.80.94	4 Core, 8 RAM, 400 Disk	
		eth1	192.168.70.84		
		eth2	103.101.161.205		
Client 1	Ubuntu 16	eth0	192.168.80.210	2 Core, 2 RAM, 50 Disk	
Client 2	Centos 7	eth0	192.168.70.93	2 Core, 4 RAM, 80 Disk	

1.2 Mô hình LAB



2. Cài đặt

2.1 Cài đặt Graylog-server

Bước 1: Thiết lập môi trường

- Thực hiện update và cài đặt gói hỗ trợ :

```
yum install -y epel-release  
yum update -y  
yum install -y git wget curl byobu  
yum install -y pwgen  
yum install -y httpd
```

- Khởi động dịch vụ http

```
systemctl start httpd  
systemctl enable httpd
```

- Tắt selinux :

```
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/sysconfig/selinux  
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
```

Bước 2 : Cài đặt NTP

- Cấu hình ntp trên cả máy Client và server :

```
yum install -y chrony
```

- Sửa file config :

Để thời gian được đồng bộ, sửa file cấu hình /etc/chrony.conf như sau :

```
server 192.168.80.82 iburst  
#server 1.centos.pool.ntp.org iburst  
#server 2.centos.pool.ntp.org iburst  
#server 3.centos.pool.ntp.org iburst
```

- Khởi động và kích hoạt chrony :

```
systemctl start chronyd  
systemctl enable chronyd
```

- Kiểm tra lại đồng bộ hóa thời gian :

```
chronyc sources
```

- Kiểm tra thời gian hệ thống :

```
timedatectl
```

Bước 3: Cài đặt Java

```
yum install -y java-1.8.0-openjdk
```

Bước 4: Cài đặt MongoDB

- Khai báo repo cho MongoDB

Tạo file `/etc/yum.repos.d/mongodb-org-4.0.repo` và khai báo nội dung như sau:

```
cat <<EOF> /etc/yum.repos.d/mongodb-org-4.0.repo
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/4.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc
EOF
```

- Cài đặt MongoDB :

```
yum install -y mongodb-org
```

- Khởi động MongoDB :

```
systemctl daemon-reload
systemctl enable mongod.service
systemctl start mongod.service
```

- Kiểm tra trạng thái của MongoDB :

```
systemctl status mongod
```

Bước 5: Cài đặt Elasticsearch

- Khai báo repo cho Elasticsearch :

Tạo file `/etc/yum.repos.d/elasticsearch.repo` và khai báo nội dung như sau:

```
cat <<EOF> /etc/yum.repos.d/elasticsearch.repo
[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

- Cài đặt Elasticsearch

```
yum install -y elasticsearch
```

- Sửa file cấu hình `/etc/elasticsearch/elasticsearch.yml` của elasticsearch như sau:

```
sed -i 's/#cluster.name: my-application/cluster.name: graylog/g'
/etc/elasticsearch/elasticsearch.yml
```

- Khởi động lại elasticsearch

```
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl restart elasticsearch.service
```

- Kiểm tra trạng thái của elasticsearch

```
systemctl status elasticsearch.service
```

Bước 6: Cài đặt graylog

- Tải về repo của graylog

```
rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-3.2-repository_latest.rpm
```

- Cài đặt graylog 3.2

```
yum install -y graylog-server
```

- Thực hiện copy file trước khi sửa file phòng khi bị lỗi

```
cp /etc/graylog/server/server.conf /etc/graylog/server/server.conf.bk
```

- Tạo chuỗi hash gồm 96 ký tự để khai báo cho `password_secret` sau đó lưu vào file cấu hình :

```
pass_secret=$(pwgen -N 1 -s 96)
sed -i -e 's|password_secret =|password_secret = '$pass_secret''|'
/etc/graylog/server/server.conf
```

- Tạo mật khẩu đăng nhập cho tài khoản admin để đăng nhập graylog :

```
echo -n nhanhoa2018@A | sha256sum
```

Sau khi tạo, mật khẩu sẽ có dạng giống như sau:

```
993f2322f02ec3ce3d7849391b6f3668134130e83d32b96074bfa29c15d051b8
```

Sau khi có được mật khẩu dưới dạng chuỗi hash, gán cho `root_password_sha2` :

```
sed -i 's|root_password_sha2 =|root_password_sha2 =
993f2322f02ec3ce3d7849391b6f3668134130e83d32b96074bfa29c15d051b8|g'
/etc/graylog/server/server.conf
```

- Sửa thời gian

```
sed -i 's|#root_timezone = UTC|root_timezone = Asia/Ho_Chi_Minh|'
/etc/graylog/server/server.conf
```

- Sửa địa chỉ IP mặc định :

```
sed -i 's|#http_bind_address = 127.0.0.1:9000|http_bind_address = 0.0.0.0:9000|'
/etc/graylog/server/server.conf
```

- Bỏ comment `root_username`

```
sed -i 's|#root_username = admin|root_username = admin|' /etc/graylog/server/server.conf
```

- Vì máy có nhiều card mạng nên cần phải chỉnh địa chỉ HTTP URI để các node khác có thể kết nối tới node graylog-server thông qua các card mạng khác nhau :

```
sed -i 's|#http_publish_uri = http://192.168.1.1:9000/|http_publish_uri = http://0.0.0.0:9000/|'
/etc/graylog/server/server.conf
```

- Khởi động dịch vụ graylog-server

```
systemctl daemon-reload
systemctl enable graylog-server.service
```

```
systemctl start graylog-server.service
```

- Kiểm tra trạng thái của graylog-server

```
systemctl status graylog-server
```

Bước 7 : Login

Login với địa chỉ **https://IP:9000** bằng user: admin và password: nhanhoa2018@A để đăng nhập vào Web interface của dịch vụ graylog.

2.2 Cấu hình thu thập log CentOS 7 thông qua graylog-sidecar

Thao tác trên c7srv01

Bước 1: Thiết lập môi trường

- Thực hiện update và cài đặt gói hỗ trợ

```
yum install -y epel-release  
yum update -y  
yum install -y git wget curl byobu  
yum install -y pwgen
```

- Tắt selinux

```
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/sysconfig/selinux  
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config  
setenforce 0
```

Bước 2: Cài đặt NTP

- Cài đặt NTP

```
yum install -y chrony
```

- Sửa file cấu hình /etc/chrony.conf để thời gian được đồng bộ :

```
server 192.168.80.82 iburst  
#server 1.centos.pool.ntp.org iburst  
#server 2.centos.pool.ntp.org iburst  
#server 3.centos.pool.ntp.org iburst
```

- Khởi động lại dịch vụ NTP

```
systemctl start chronyd  
systemctl enable chronyd
```

- Kiểm tra lại đồng bộ :

```
chronyc sources
```

- Kiểm tra lại thời gian :

```
timedatectl
```

Bước 3: Cài đặt Sidecar và filebeat

Cài đặt file Beats

- Tải về file Beats

Để cài file Beats ta cần tìm và tải về phiên bản hệ điều hành thích hợp, phiên bản này là CentOS 7 nên sẽ sử dụng phiên bản sau :

```
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.2-x86\_64.rpm
```

- Cài đặt file Beats

```
rpm -i filebeat-7.4.2-x86_64.rpm
```

Cài đặt graylog-sidecar

- Tiến hành tải về

```
wget  
https://github.com/Graylog2/collector-sidecar/releases/download/1.0.2/graylog-sidecar-1.0.2-1.x86\_64.rpm
```

- Cài đặt file graylog-sidecar :

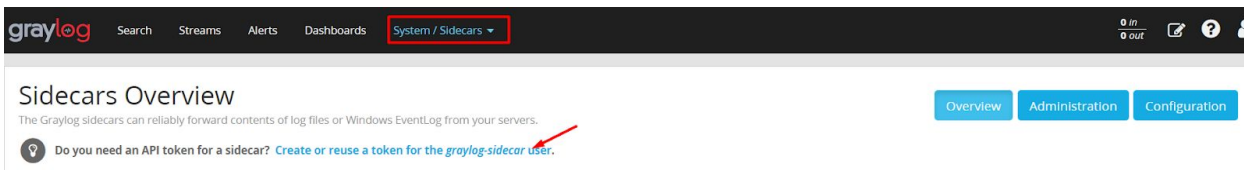
```
rpm -i graylog-sidecar-1.0.2-1.x86_64.rpm  
graylog-sidecar -service install
```

Lưu ý: Để cấu hình sidecar, trước tiên ta cần đăng nhập vào Web Interface của graylog để tạo và lấy Token. Một mã token có thể dùng chung cho nhiều client, tuy

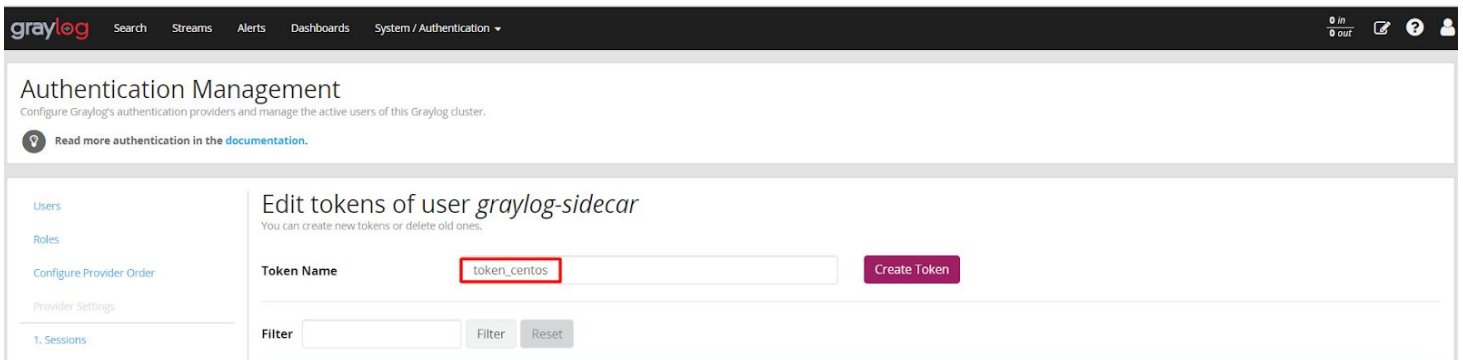
nhiên ở đây mình sử dụng token theo nhóm client ví dụ (token_centos, token_ubuntu, token_windows ..).

Dưới là bước tạo token lần đầu tiên để sử dụng cho bước khai báo phía client.

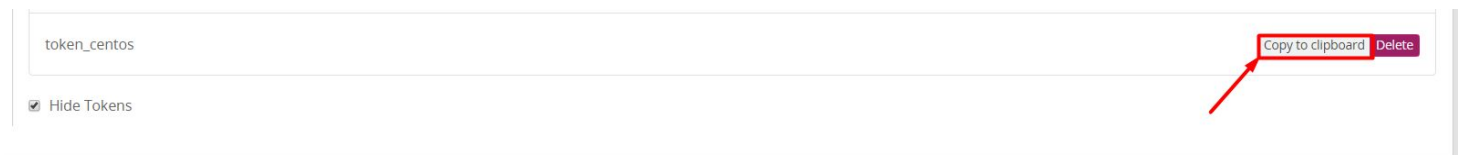
- Vào Web Interface của graylog, truy cập tab System/Sidecars , sau đó chọn Create or reuse a token for the graylog-sidecar user :



- Nhập tên và chọn Create Token để tạo token, nên tạo tên token theo nhóm để gọi nhớ và sử dụng chung.



- Sau đó ta copy mã token để sử dụng cho việc cấu hình graylog-sidecar :



- Mã token có dạng như sau:

157vjbs3t175upg3id65gb6k2nhj0v8k2k17j51g057ed8h9rl4

Lưu ý: Nếu muốn lấy mã token đã tạo trước đó, ta có thể thực hiện các bước như tạo token, sau đó tìm mã token sẵn có và copy.

Quay lại máy Graylog-sidecar (c7srv01) để chỉnh sửa file config, các thao tác sửa đổi được thực hiện ở file `/etc/graylog/sidecar/sidecar.yml` :

- Trước khi sửa file ta nên thực hiện copy file ra phòng khi có lỗi
`cp /etc/graylog/sidecar/sidecar.yml /etc/graylog/sidecar/sidecar.yml.bk`

- Khai báo ip của graylog-server:

```
sed -i 's|#server_url: "http://127.0.0.1:9000/api/"|server_url: "http://192.168.70.84:9000/api/"|' /etc/graylog/sidecar/sidecar.yml
```

Lưu ý: Địa chỉ ip 192.168.70.84 được sử dụng trong trường hợp các client cùng vlan với 192.168.70.0/24. Các client thuộc vlan khác cần thay địa chỉ sao cho đúng.

- Thay giá trị `api_token` bằng chuỗi token đã tạo trước đó :

```
sed -i 's|server_api_token: ""|server_api_token: "157vjbs3t175upg3id65gb6k2nhj0v8k2k17j51g057ed8h9rl4"|' /etc/graylog/sidecar/sidecar.yml
```

- Sửa đổi và bỏ comment 1 số dòng để graylog-sidecar hoạt động :

```
sed -i 's|#log_path: "/var/log/graylog-sidecar"|log_path: "/var/log/graylog-sidecar"|' /etc/graylog/sidecar/sidecar.yml
```

```
sed -i 's|#tls_skip_verify: false|tls_skip_verify: true|' /etc/graylog/sidecar/sidecar.yml
```

- Bỏ comment và sửa `node_name` như sau (sửa `node_name` theo tên của client):

```
sed -i 's|#node_name: ""|node_name: "c7srv01"|' /etc/graylog/sidecar/sidecar.yml
```

- Tiến hành khởi động dịch vụ graylog-sidecar :

```
systemctl start graylog-sidecar.service
```

```
systemctl enable graylog-sidecar.service
```

- Kiểm tra lại trạng thái graylog-sidecar.

```
systemctl status graylog-sidecar.service
```

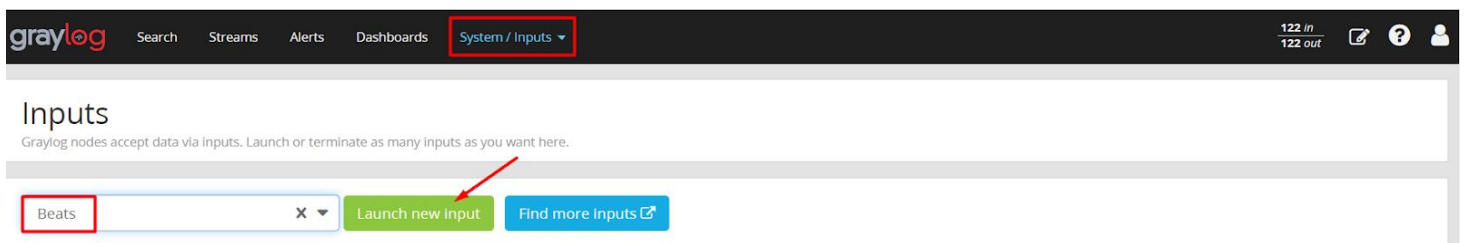
- Nếu không thể khởi động dịch vụ graylog-sidecar, ta cần xem lại sửa đổi trong file config của graylog-sidecar xem sửa đổi đã giống bên dưới chưa `cat /etc/graylog/sidecar/sidecar.yml | egrep -v "^*#|^$"`. Nếu chưa giống thì sửa lại cho giống với hình dưới sau đó tiến hành khởi động lại dịch vụ graylog.

```
[root@c7srv01 ~]# cat /etc/graylog/sidecar/sidecar.yml | egrep -v "^*#|^$"
server_url: "http://192.168.70.84:9000/api/"
server_api_token: "157vjbs3t175upg3id65gb6k2nhj0v8k2k17j51g057ed8h9rl4"
node_name: "c7srv01"
update_interval: 10
tls_skip_verify: true
log_path: "/var/log/graylog-sidecar"
```

Bước 4 : Cấu hình Sidecar trên Web Interface của graylog-server

Khai báo input cho Sidecar :

- Để graylog-server biết nơi cần nhận log, ta cần khai báo input cho graylog-server. Truy cập System/Inputs và chọn input là Beats và bấm Launch new input :



- Tiếp đến ta edit input như sau :

☒ Global

Should this input start on all nodes

Title

Beats_70

Bind address

192.168.70.84

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

5044

Port to listen on.

Receive Buffer Size (optional)

1048576

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

No. of worker threads (optional)

4

- Sau đó tích vào mục `Do not add Beats type as prefix` lưu lại phần cấu hình :

The password for the encrypted key file.

TLS client authentication (optional)

Whether clients need to authenticate themselves in a TLS connection

TLS Client Auth Trusted Certs (optional)

TLS Client Auth Trusted Certs (File or Directory)

☐ TCP keepalive

Enable TCP keepalive packets

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.

☒ Do not add Beats type as prefix

Do not prefix each field with the Beats type, e. g. "source" -> "filebeat_source".

Cancel

Save

- Sau khi tạo, ta có được input của file beats như sau:

Filter

Reset

Global inputs 1 configured

Beats_70 Beats 1 RUNNING

```
bind_address: 192.168.70.84
no_beats_prefix: false
number_worker_threads: 4
override_source: <empty>
port: 5044
recv_buffer_size: 1048576
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password:*****
```

Cấu hình Sidecars

- Truy cập vào System/Sidecar chọn Configuration sau đó chọn Create Configuration :



- Khai báo các thông số và sửa địa chỉ ip thành địa chỉ của graylog-server. Ở đây ta chỉ lấy ssh nên ta xóa hết những nguồn log khác và chỉ để /var/log/secure và bổ sung trường `fields.source: ${sidecar.nodeName}`

Name

LAN 70

Required. Name for this configuration

Configuration color



Change color

Choose a color to use for this configuration.

Collector

filebeat on Linux

Note: Log Collector cannot change while the Configuration is in use. Clone the Configuration to test it using another Collector.

Configuration

```
1 # Needed for Graylog
2 fields_under_root: true
3 fields.collector_node_id: ${sidecar.nodeName}
4 fields.gl2_source_collector: ${sidecar.nodeId}
5 fields.source: ${sidecar.nodeName}
6
7 filebeat.inputs:
8 - input_type: log
9   paths:
10    - /var/log/secure
11   type: log
12 output.logstash:
13   hosts: ["192.168.70.84:5044"]
14 path:
15   data: /var/lib/graylog-sidecar/collectors/filebeat/data
16   logs: /var/lib/graylog-sidecar/collectors/filebeat/log
```

Required. Collector configuration, see quick reference for more information.

Migrate Preview

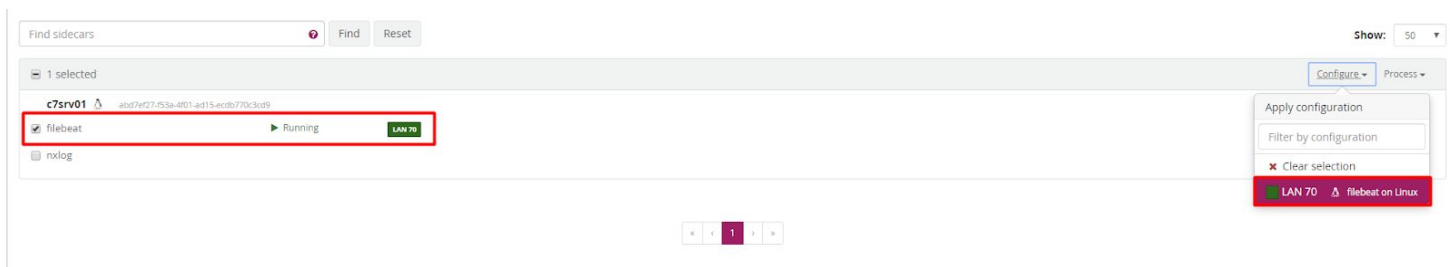
Update

Back

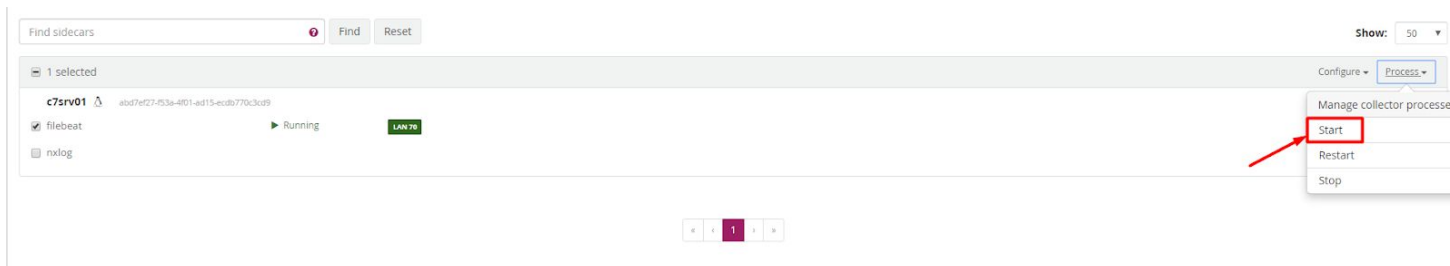
- Tiếp đến, chọn tab Administration



- Tích chọn filebeat Sau đó chọn configuration vừa tạo là LAN 70 :



- Tiếp đến chọn Process -> Start để khởi động trình thu thập log từ c7srv01, có một cửa sổ bật lên, chọn Confirm để tiếp tục.

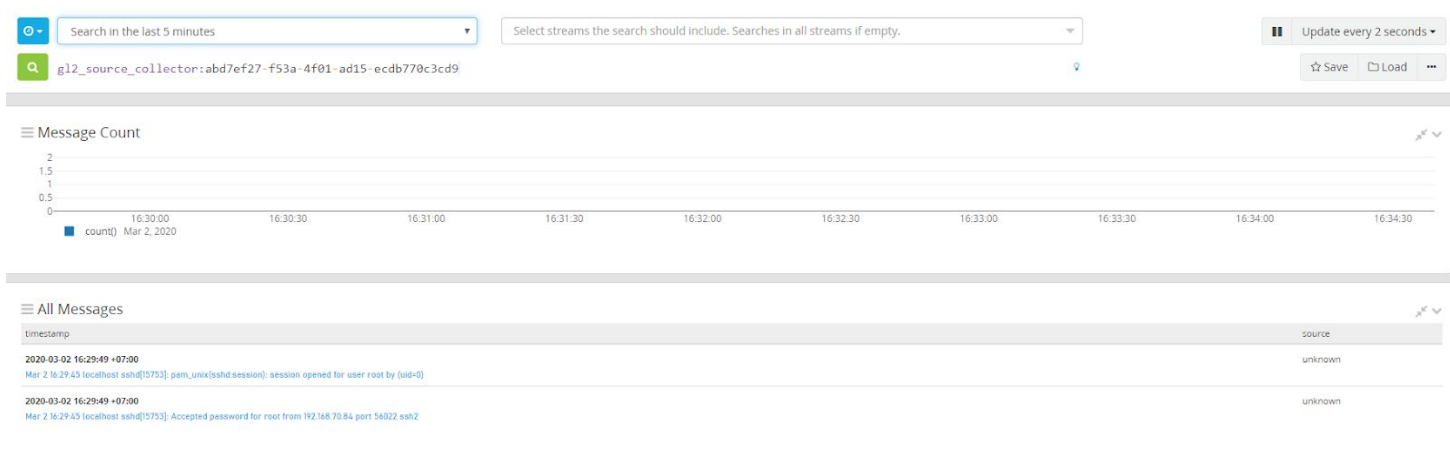


Kiểm tra kết quả

Chuyển sang tab Overview và chọn Show messages



Sau đó ssh vào máy c7srv01 để kiểm tra log gửi về :



Có log đầy về như hình trên là đã cài thành công.

2.3 Cấu hình thu thập log Ubuntu 16 thông qua graylog-sidecar

Bước 1: Thiết lập môi trường :

Đăng nhập với quyền root hoặc sử dụng sudo để thực hiện các bước cài đặt.

- Thực hiện update và cài đặt gói bổ trợ.

```
apt-get -y update
```

```
apt-get install -y git vim byobu
```

- Thiết lập NTP :

Cài đặt dịch vụ ntp :

```
apt install chrony
```

Thực hiện sửa file config của dịch vụ ntp tại `/etc/chrony/chrony.conf` , thêm dòng sau vào file cấu hình :

```
server 192.168.80.82
```

Lưu ý: Địa chỉ 192.168.80.82 là địa chỉ máy chủ NTP của hệ thống này. Thay bằng địa chỉ máy chủ NTP hệ thống của bạn.

Khởi động lại dịch vụ ntp :


```
systemctl restart chrony
```

Kiểm tra lại đồng bộ và kiểm tra thời gian hệ thống :

```
chronyc sources
```

```
timedatectl
```

Bước 2: Cài đặt graylog-sidecar và filebeat

- Cài đặt filebeat

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee  
/etc/apt/sources.list.d/elastic-7.x.list
```

```
apt-get install -y apt-transport-https
```

```
apt-get update -y
```

```
apt-get install -y filebeat
```

- Cài đặt graylog-sidecar

Thực hiện tải bộ cài graylog-sidecar

```
cd /root
```

```
wget
```

```
https://github.com/Graylog2/collector-sidecar/releases/download/1.0.2/graylog-sidecar\_1.0.2-1  
\_amd64.deb
```

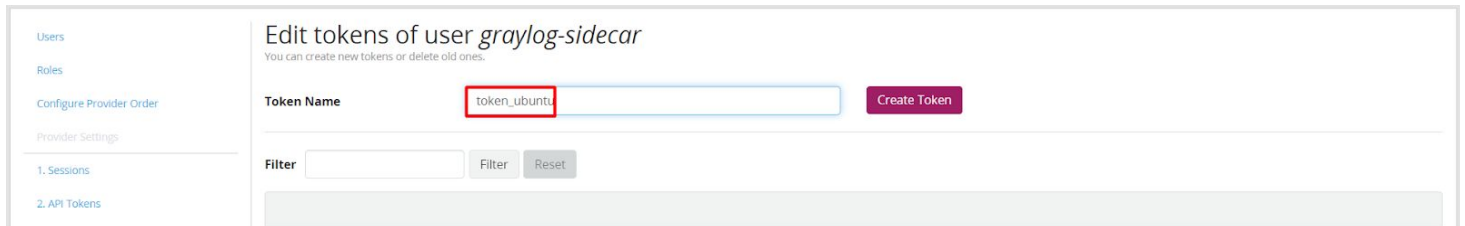
Tiến hành cài graylog-sidecar

```
sudo dpkg -i graylog-sidecar_1.0.2-1_amd64.deb
```

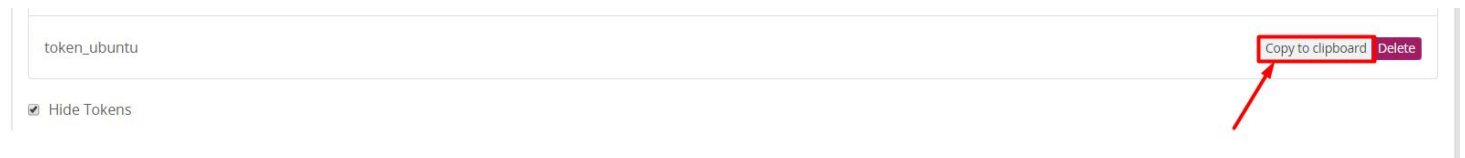
Cũng như cách cấu hình thu thập log của CentOS 7, ta cũng phải đăng nhập vào Web Interface của graylog-server để lấy 1 mã Token.

Lưu ý: Một mã token có thể dùng chung cho nhiều client, tuy nhiên ở đây mình sử dụng token theo nhóm client ví dụ (token_centos, token_ubuntu, token_windows ..). Trong quá trình triển khai nên tìm những token đã tạo trước đó, không cần tạo mới token

- Đăng nhập vào Graylog-server, sau đó truy cập tab System/Sidecars, chọn dòng Create a token for the graylog-sidecar user. Nhập tên Token và bấm vào Create Token để tạo.



- Sau đó copy mã Token và lưu lại để dùng ở bước sau:



- Dòng Token đối với bài lab này có dạng như sau:

186hti76hj9upg3id65gb6k2nhj0v8k6y9i5y8g057ed8h9rl4

Trở lại máy graylog-sidecar, vào file /etc/graylog/sidecar/sidecar.yml và sửa những dòng sau:

- Tiến hành copy file config phòng trường hợp cấu hình gặp vấn đề:

```
cp /etc/graylog/sidecar/sidecar.yml /etc/graylog/sidecar/sidecar.yml.bk
```

- Khai báo IP của graylog-server

```
server_url: "http://192.168.80.94:9000/api/"
```

Lưu ý: Nếu IP là private, IP của Client ở dải nào thì khai báo đúng IP của server ở dải đó.

- Khai báo Token mới tạo ở dòng `server_api_token` :

```
server_api_token: "186hti76hj9upg3id65gb6k2nhj0v8k6y9i5y8g057ed8h9rl4"
```

- Sửa `node_name` để khai báo hostname của client (sửa `node_name` theo tên của máy) :

```
node_name: "U16SRV02"
```

- Bỏ comment `list_log_files` và sửa `/var/log/nginx` thành :

```
list_log_files:  
  - "/var/log/"
```

- Tìm và bỏ comment những dòng sau :

```
node_id: "file:/etc/graylog/sidecar/node-id"
```

```
update_interval: 10
```

```
cache_path: "/var/cache/graylog-sidecar"
```

```
log_path: "/var/log/graylog-sidecar"
```

- Sau khi sửa file, kiểm tra lại dữ liệu đã sửa bằng lệnh sau:

```
root@U16SRV02:~# cat /etc/graylog/sidecar/sidecar.yml | egrep -v "^*#|^$"
server_url: "http://192.168.80.94:9000/api/"
server_api_token: "186hti76hj9upg3id65gb6k2nhj0v8k6y9i5y8g057ed8h9rl4"
node_id: "file:/etc/graylog/sidecar/node-id"
node_name: "U16SRV02"
update_interval: 10
list_log_files:
  - "/var/log/"
cache_path: "/var/cache/graylog-sidecar"
log_path: "/var/log/graylog-sidecar"
```

- Sau khi kiểm tra, khởi động và kích hoạt graylog-sidecar:

```
graylog-sidecar -service install
```

```
systemctl start graylog-sidecar
```

```
systemctl enable graylog-sidecar
```

- Kiểm tra lại trạng thái của graylog-sidecar:

```
systemctl status graylog-sidecar
```

Bước 3: Cấu hình sidecar trên Graylog-server :

Khai báo input cho U16SRV02

Input này có thể sử dụng chung cho các máy trong cùng 1 dải mạng.

- Truy cập `System/Inputs` , kích chọn `Beats` sau đó chọn `Launch new input` :



- Tiếp theo, ta điền các mục cần thiết để khai báo input :

☒ Global

Should this input start on all nodes

Title

Beats_80

Bind address

192.168.80.94

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

5044

Port to listen on.

Receive Buffer Size (optional)

1048576

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

No. of worker threads (optional)

4

- Sau đó tích chọn **Do not add Beats type as prefix** và bấm **Save** để lưu lại.

The password for the encrypted key file.

TLS client authentication (optional)

Whether clients need to authenticate themselves in a TLS connection

TLS Client Auth Trusted Certs (optional)

TLS Client Auth Trusted Certs (File or Directory)

☐ TCP keepalive

Enable TCP keepalive packets

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.

☒ Do not add Beats type as prefix

Do not prefix each field with the Beats type, e. g. "source" -> "filebeat_source".

Cancel

Save

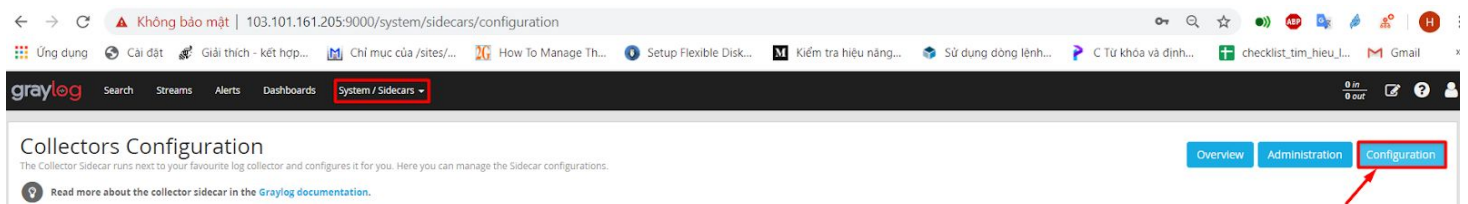
- Kết quả sau khi khai báo sẽ trông như sau:

Beats_80 Beats **1 RUNNING**

```
bind_address: 192.168.80.94
no_beats_prefix: false
number_worker_threads: 4
override_source: <empty>
port: 5044
recv_buffer_size: 1048576
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password:*****
```

Cấu hình sidecar

- Truy cập tab System/Sidecars chọn Configuration :



- Chọn Create Configuration




- Ta sẽ tạo 1 Configuration để dùng chung cho IP ở dải 80 :

Name

LAN 80

Required. Name for this configuration.

Configuration color

 [Change color](#)

Choose a color to use for this configuration.

Collector

filebeat on Linux

Note: Log Collector cannot change while the Configuration is in use. Clone the Configuration to test it using another Collector.

Configuration

```
1 # Needed for Graylog
2 fields_under_root: true
3 fields.collector_node_id: ${sidecar.nodeName}
4 fields.gl2_source_collector: ${sidecar.nodeId}
5 fields.source: ${sidecar.nodeName}
6
7 filebeat.inputs:
8   - input_type: log
9     paths:
10      - /var/log/auth.log
11      type: log
12 output.logstash:
13   hosts: ["192.168.80.94:5044"]
14 path:
15   data: /var/lib/graylog-sidecar/collectors/filebeat/data
16   logs: /var/lib/graylog-sidecar/collectors/filebeat/log
```

Required. Collector configuration, see quick reference for more information.

[Migrate](#) [Preview](#)

[Update](#) [Back](#)

Lưu ý:- Dòng 5 để log hiển thị tên của máy graylog-sidecar.

- Dòng 10 để thu thập log ssh của Ubuntu, nếu thu thập thêm log của CentOS 7 thì ta phải chỉ định thêm đường dẫn file log ssh của CentOS 7 là:
/var/log/secure

- Dòng 12 khai báo địa chỉ ip của graylog-server.

- Sau khi điền các thông tin cần thiết, lưu lại cấu hình và chuyển sang tab Overview.

Sidecars Overview

The Graylog sidecars can reliably forward contents of log files or Windows EventLog from your servers.

Do you need an API token for a sidecar? [Create or reuse a token for the graylog-sidecar user.](#)

Find sidecars Show: 50

Name	Status	Operating System	Last Seen	Node Id	Sidecar Version
U16SRV02	Running	Linux	a few seconds ago	555e7911-aeec-4c3f-a141-cdb7f1b33861	1.0.2
c7srv01	Running	Linux	a few seconds ago	abd7ef27-f53a-4f01-ad15-ecdb770c3cd9	1.0.2

< 1 >

- Chọn Manage sidecars ở máy cần cấu hình, ở đây là máy U16SRV02 :

Sidecars Overview

The Graylog sidecars can reliably forward contents of log files or Windows EventLog from your servers.

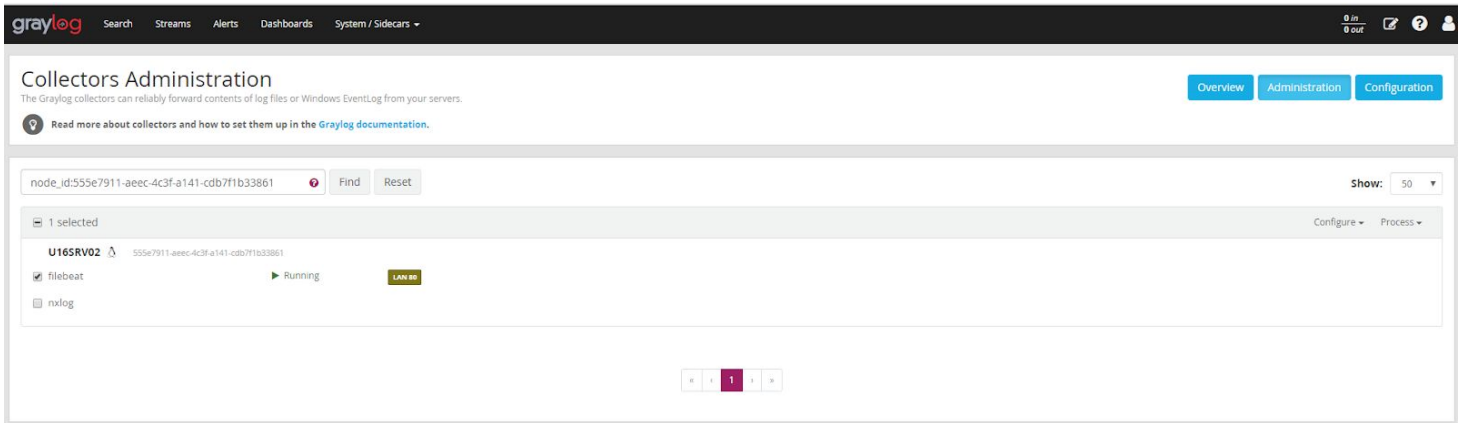
Do you need an API token for a sidecar? [Create or reuse a token for the graylog-sidecar user.](#)

Find sidecars Show: 50

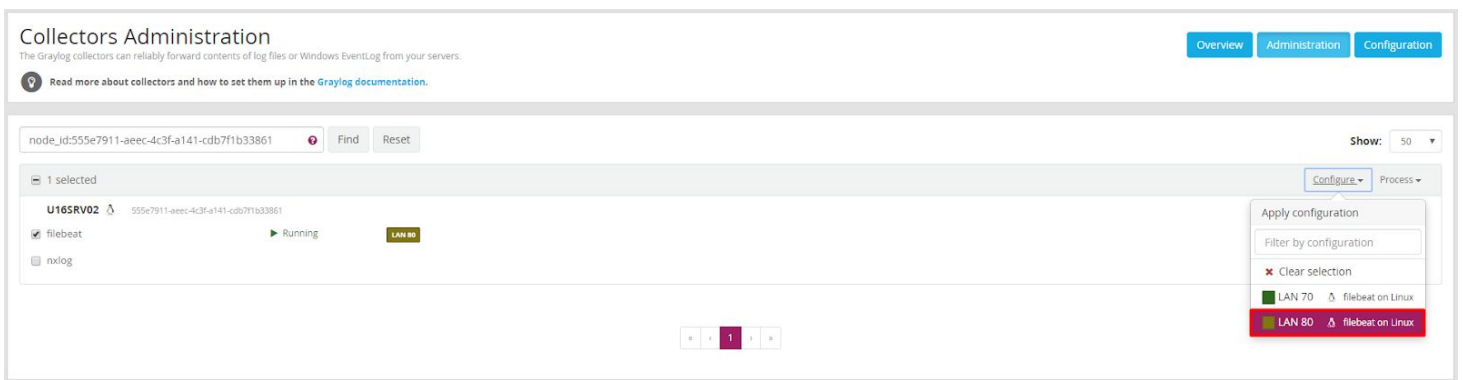
Name	Status	Operating System	Last Seen	Node Id	Sidecar Version
U16SRV02	Running	Linux	a few seconds ago	555e7911-aeec-4c3f-a141-cdb7f1b33861	1.0.2
c7srv01	Running	Linux	a few seconds ago	abd7ef27-f53a-4f01-ad15-ecdb770c3cd9	1.0.2

< 1 >

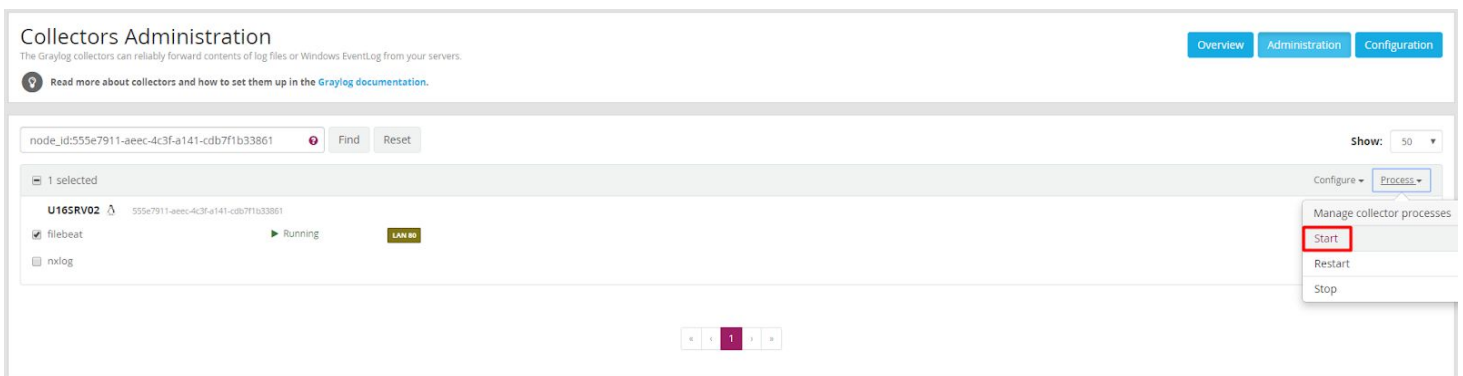
- Tiếp đến, tích chọn filebeats :



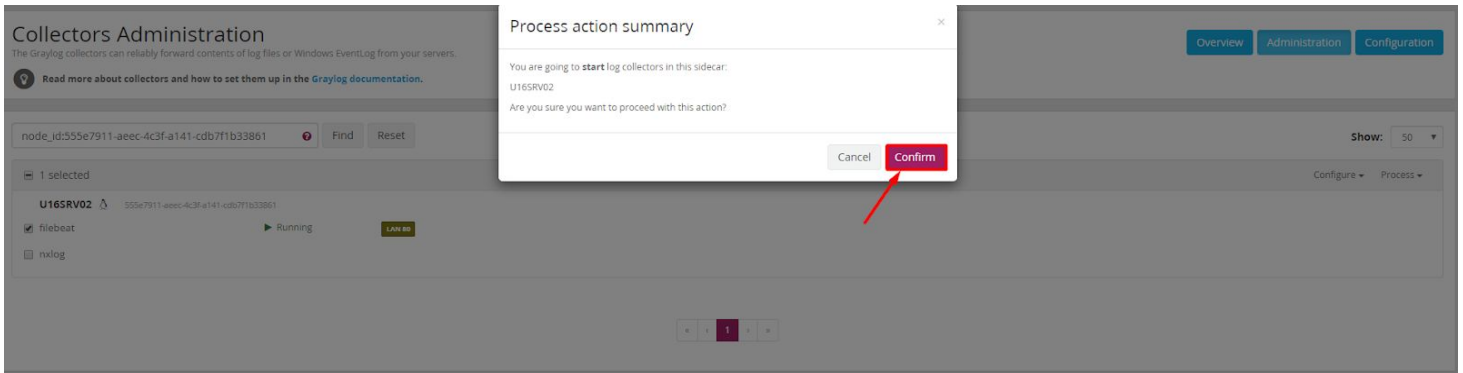
- Chọn **Configuration** là **LAN 80**, một cửa sổ bật lên **Confirm** để xác nhận.



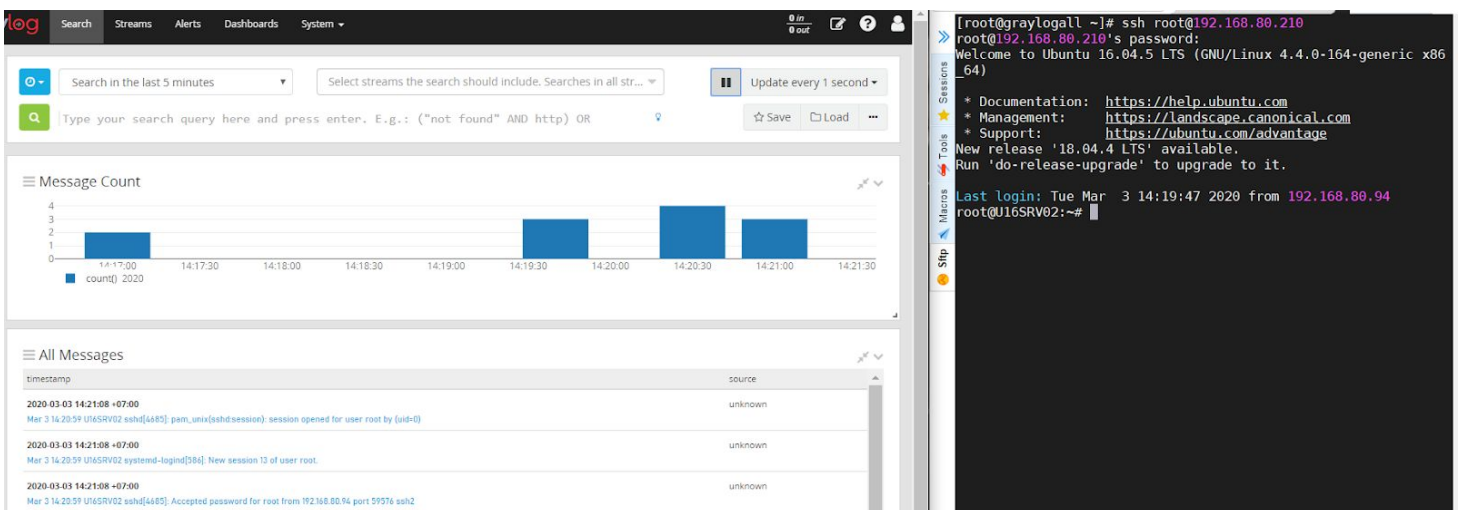
- Sau khi xác nhận, tiếp tục chọn **Process** và chọn **Start** để bắt đầu.



- Chọn **Confirm**



- Kiểm tra lại log gửi về :



Sau khi thực hiện ssh, đã có log gửi về. Như vậy là đã cấu hình thành công.

3. Cấu hình cảnh báo và cấu hình Dashboards

3.1 Cấu hình và cài đặt Telegram, Slack, Email

Bước 1: Cấu hình cảnh báo Telegram

Tạo Bot telegram và add Bot và Group trong Telegram

- Sử dụng BotFather để tạo 1 Bot trong telegram, sau khi tạo Bot sẽ có 1 API Token. Copy Token đó và lưu lại để dùng sau.
- Sau khi đã tạo Bot, ta add Bot vào group trong Telegram, thực hiện lấy ID của group và lưu lại.
- Các bước tạo Bot và add vào group có thể tham khảo [tại đây](#).
- Sau khi đã có ID của group và Token của Bot, ta thực hiện cấu hình cảnh báo về telegram trên graylog-server.

Truy cập vào Graylog-server để tải về và cài đặt telegram.

- Di chuyển đến thư mục plugin của graylog:

```
cd /usr/share/graylog-server/plugin/
```

- Tải về plugin của Telegram :

```
wget
```

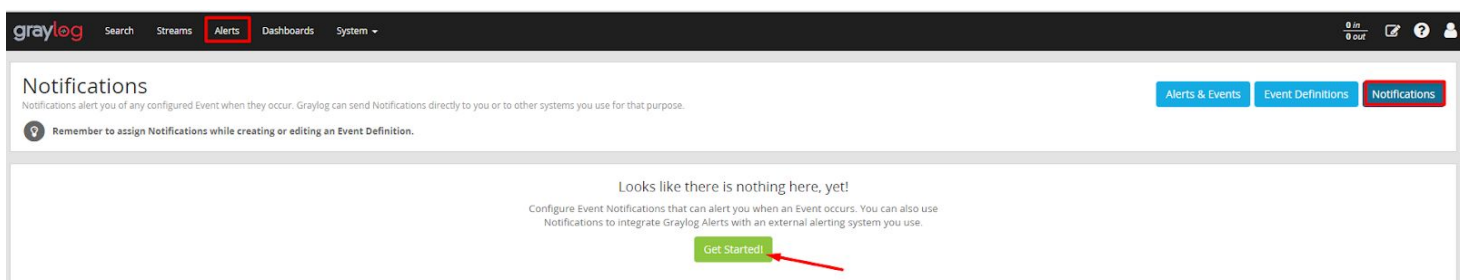
```
https://github.com/irgendwr/TelegramAlert/releases/download/v2.2.0/telegram-alert-2.2.0.jar
```

- Khởi động lại dịch vụ graylog-server :

```
systemctl restart graylog-server
```

- Truy cập vào Web Interface của graylog bằng tài khoản admin.

Vào mục Alerts , chọn tab Notifications sau đó kích chọn Get Started để tạo 1 thông báo mới.



- Điền các thông số cấu hình cần thiết. Các trường bắt buộc là Title, Notification Type, Choose Legacy Notification, lưu ý các mục sao cho đúng với mục đích cấu hình.

Title
Alerts Telegram

Title to identify this Notification.

Description (Optional)
Gửi cảnh báo về group trong telegram

Longer description for this Notification.

Notification Type
Legacy Alarm Callbacks

Notification config type cannot be empty.

Choose Legacy Notification
Legacy Telegram Alert

Select a Legacy Notification to use on this Event Definition.

Legacy alarm callbacks are deprecated. Please switch to the new notification types as soon as possible!

Message

```
<a href="${stream_url}">${stream_title}</a>: ${alert_condition_title}
<code>${foreach backlog message}
  ${message.message}
${end}</code>
```

- Điền chat IDs của group, Bot Token và URL địa chỉ Web Interface của graylog-server. Sau đó chọn Execute Test Notification để thử nghiệm 1 tin nhắn gửi về group trên telegram.

Chat IDs
-407238775

You can enter multiple, comma-separated chat IDs.

Parse Mode
HTML

See <https://core.telegram.org/bots/api#formatting-options> for more information on formatting.

Bot Token
[redacted]

HTTP API Token from @BotFather

Graylog URL
http://103.101.161.205:9000/

URL to your Graylog web interface. Used to build links in alarm notification.

Proxy (optional)
[empty]

Proxy address in the following format: <ProxyAddress>:<Port>

Test Notification (Optional)
Execute Test Notification

Execute this Notification with 'Test Alert'.

Create Cancel

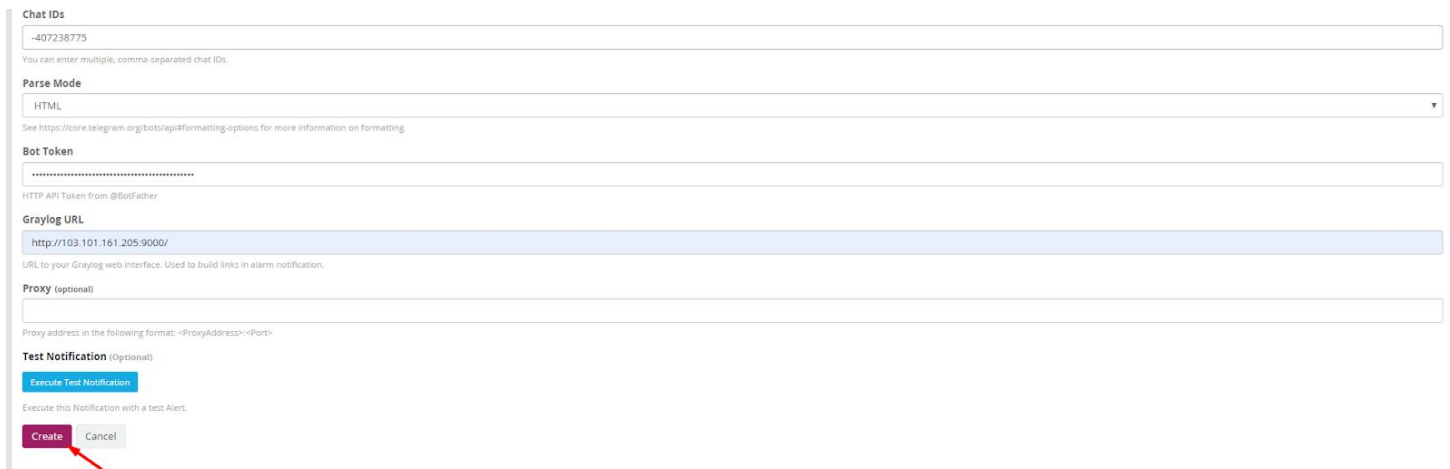
- Khi có tin nhắn gửi về group có nghĩa là đã thành công .



NH_LOG_BOT

Missing stream: Event Definition Test Title

- Chọn **Create** để khởi tạo thông báo.



Chat IDs

-407238775

You can enter multiple, comma-separated chat IDs.

Parse Mode

HTML

See <https://core.telegram.org/bots/api#formatting-options> for more information on formatting.

Bot Token

HTTP API Token from @BotFather

Graylog URL

<http://103.101.161.205:9000/>

URL to your Graylog web interface. Used to build links in alarm notification.

Proxy (optional)

Proxy address in the following format: <ProxyAddress>:<Port>

Test Notification (Optional)

Execute Test Notification

Execute this Notification with a test Alert.

Create Cancel

Bước 2: Cấu hình cảnh báo Email

- Cài đặt và cấu hình postfix trên graylog-server.

Các bước cài đặt postfix trên graylog-server có thể tham khảo [tại đây](#) !

- Vào file config của Postfix vi `/etc/postfix/main.cf` và thêm vào cuối file nội dung sau:

```
myhostname = hostname.example.com

relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

- Tạo file thông tin xác thực tài khoản mật khẩu SASL vi `/etc/postfix/sasl_passwd` và thêm thông tin như sau:

```
[smtp.gmail.com]:587 username:password
```

Lưu ý: Phần username và password sẽ thay bằng tài khoản và mật khẩu của email. Đảm bảo là đã tắt cảnh báo đăng nhập của email để không xảy ra lỗi.

- Tiến hành phân quyền cho file :

```
postmap /etc/postfix/sasl_passwd  
chown root:postfix /etc/postfix/sasl_passwd*  
chmod 640 /etc/postfix/sasl_passwd*  
systemctl reload postfix
```

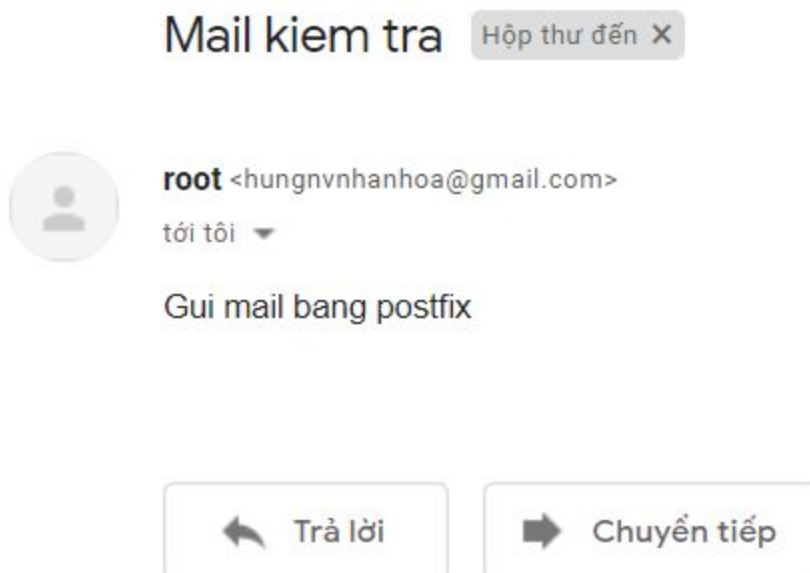
- Khởi động lại dịch vụ

```
systemctl restart postfix  
systemctl enable postfix
```

- Kiểm tra lại xem mail đã thành công hay chưa :

```
echo "Gui mail bang postfix" | mail -s "Mailkiem tra" <địa chỉ email người nhận>
```

- Nếu mail trả về như này là đã thành công :



- Tiếp theo, thêm phần cấu hình sau vào cuối file `/etc/graylog/server/server.conf` :

```
transport_email_enabled = true
transport_email_hostname = smtp.gmail.com
transport_email_port = 587
transport_email_use_auth = true
transport_email_auth_username = your_mail@gmail.com
transport_email_auth_password = your_password
transport_email_subject_prefix = [graylog]
transport_email_from_email = your_mail@gmail.com
transport_email_use_tls = true
transport_email_use_ssl = false
```

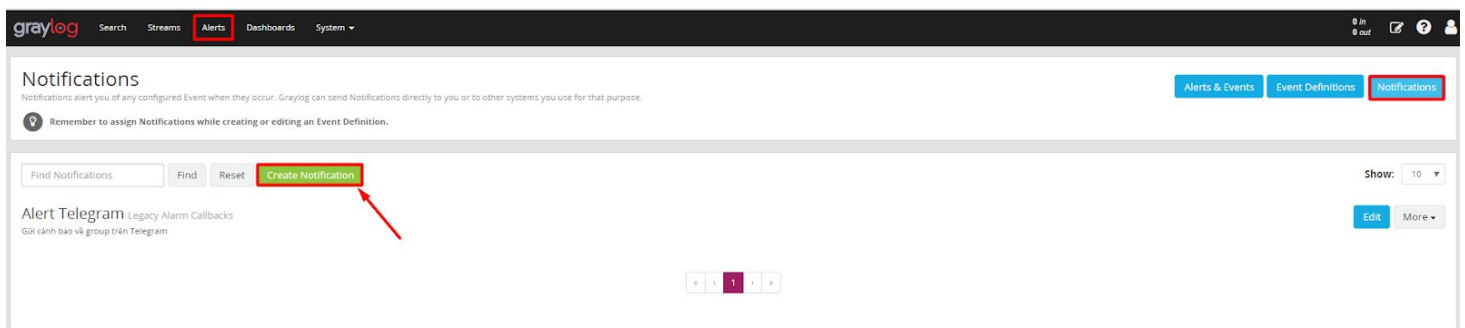
Lưu ý: Ta cần sửa email và mật khẩu ở mục `transport_email_auth_username`, `transport_email_from_email` và `transport_email_auth_password` cho giống với email và password trong file sasl. Mục `transport_email_auth_username` và `transport_email_from_email` nhập giống nhau.

- Lưu lại thay đổi và khởi động lại dịch vụ graylog-server

```
systemctl restart graylog-server
```

- Truy cập vào Web Interface

Kích vào **Alert**, chọn tab **Notifications** và click vào **Create Notification** :



- Điền thông tin vào các trường như bên dưới :

Title

 Title to identify this Notification.

Description (Optional)

 Longer description for this Notification.

Notification Type

 Choose the type of Notification to create.

Sender

 The email address that should be used as the notification sender.

Subject

 The subject that should be used for the email notification.

User recipient(s) (Optional)

- Click vào **Execute Test Notification** để test thông báo trước, 1 trạng thái trả về là **Success**: Notification was executed successfully là đã thành công.

User recipient(s) (Optional)

 Select Graylog users that will receive this Notification.

Email recipient(s) (Optional)

 Add email addresses that will receive this Notification.

Body Template

```

13 Timerange Start:    ${event.timerange_start}
14 Timerange End:     ${event.timerange_end}
15 Fields:
16 ${foreach event.fields field} ${field.key}: ${field.value}
17 ${end}
18 ${if backlog}
19 --- [Backlog] -----
20 Last messages accounting for this alert:
21 ${foreach backlog message}++
22 ${message}
23 ${end}
24 ${end}
25
  
```

The template that will be used to generate the email body.

Test Notification (Optional)

 Execute this Notification with a Test Alert.

Lưu ý:

- Mục sender để nhập email gửi đi (người gửi) cũng là email đăng nhập trong graylog-server.
- Email recipient(s) để nhập email của 1 hoặc 1 nhóm người nhận.
- Body Template sẽ là phần body của email khi gửi về.

- Sau khi điền các thông số và thực hiện test email, chọn **update** để cập nhật cấu hình cảnh báo mail.

Body Template

```

1 --- [Event Definition] -----
2 Title:      ${event_definition_title}
3 Description: ${event_definition_description}
4 Type:       ${event_definition_type}
5 --- [Event] -----
6 Timestamp:  ${event.timestamp}
7 Message:    ${event.message}
8 Source:     ${event.source}
9 Key:        ${event.key}
10 Priority:   ${event.priority}
11 Alert:     ${event.alert}
12 Timestamp Processing: ${event.timestamp}
13 Timerange Start:  ${event.timerange_start}

```

The template that will be used to generate the email body.

Test Notification (Optional)

[Execute Test Notification](#)

Success: Notification was executed successfully.

Execute this Notification with a test Alert.

[Update](#) [Cancel](#)

Bước 3: Cấu hình cảnh báo Slack

- Di chuyển đến thư mục plugin của Graylog-server.

```
cd /usr/share/graylog-server/plugin/
```

- Truy cập địa chỉ và copy đường link download plugin phù hợp với phiên bản graylog-server

<https://github.com/graylog-labs/graylog-plugin-slack/releases>

- Tải về plugin của slack

```
wget
```

```
https://github.com/graylog-labs/graylog-plugin-slack/releases/download/3.1.0/graylog-plugin-slack-3.1.0.jar
```

- Khởi động lại dịch vụ graylog-server

```
systemctl restart graylog-server
systemctl status graylog-server
```

- Trên kênh slack tạo 1 channel có tên là graylog

R&D ▾



● Nguyễn Việt Hùng

☰ Accéder à...

⋮ Applications

Chaînes



aléatoire

général

🔒 graylog

openstack

+ Ajouter une chaîne

Messages directs



♥ Slackbot

● Nguyễn Việt Hùng (vous)

○ hungnvnhanhoa


● Niemdt

+ Inviter des personnes

Applications récentes

+ Installer Google Calendar

- Sau đó copy link của không gian làm việc :

**Nguyễn Việt Hùng**


[Définir un statut](#) Ctrl+Shift+Y

[Profil et compte](#)

[Préférences](#)

[Me signaler **absent\(e\)**](#)

[Aide et commentaires](#)

**R&D**

[rd-qzi2537.slack.com](#)

Votre espace de travail utilise actuellement la version gratuite de Slack.

[Voir les options de mise à niveau](#)

[Administration](#)

[Inviter des personnes](#)

[Analyse des données](#)

[Personnaliser Slack](#)

[Chaînes partagées](#)

[Se déconnecter de **R&D**](#)

[Ouvrir l'application Slack](#)

- Truy cập địa chỉ sau với <organization> là link vừa copy.

`https://<organization>/apps/new/A0F7XDUAZ-webhooks-entrants`

- Chọn channel là graylog vừa tạo và tích hợp thêm Webhooks đến.

slack App Directory

Rechercher des applications

Parcourir Gérer Créer R&D

Parcourir les applications > Intégrations personnalisées > Webhooks entrants > Nouvelle configuration

Webhooks entrants

Send data into Slack in real-time.

Webhooks đến là một cách đơn giản để gửi tin nhắn từ các nguồn bên ngoài vào Slack. Họ sử dụng các yêu cầu HTTP thông thường với tải trọng JSON, bao gồm thông báo và một vài chi tiết tùy chọn khác được mô tả sau.

Phần đính kèm tin nhắn cũng có thể được sử dụng trong Webhooks đến để hiển thị các tin nhắn có định dạng phong phú, nổi bật so với các tin nhắn trò chuyện thông thường.

Vous découvrez les intégrations Slack ?
Consultez notre guide [Premiers pas](#) pour vous familiariser avec les types d'intégration les plus courants et pour trouver des conseils dont vous tiendrez compte en créant la vôtre. Si vous le souhaitez, [register as a developer](#) (inscrivez-vous en tant que développeur) pour nous faire connaître le projet sur lequel vous travaillez et recevoir les mises à jour futures de nos API.

Publier dans la chaîne
Commencez par choisir une chaîne dans laquelle votre webhook entrant publiera des messages.

graylog

ou créer une chaîne

Ajouter l'intégration Webhooks entrants

En créant un webhook entrant, vous acceptez les [Conditions d'utilisation des API](#) Slack.

- Sau đó ta sẽ có được URL Webhooks, copy và note lại để sau sử dụng cho việc gửi cảnh báo về channel.

Parcourir les applications > Intégrations personnalisées > Webhooks entrants > Modifier la configuration



Webhooks entrants

Ajouté par Nguyễn Việt Hùng le 4 mars 2020

Désactiver • Supprimer

Webhooks sont un moyen simple de recevoir des données de sources externes dans Slack. Ils utilisent des appels HTTP standards avec des données au format JSON, y compris des notifications et des données structurées choisies décrites ci-dessous.

Les **webhooks entrants** peuvent également être utilisés pour afficher des données structurées, notamment les données de type **notification**.



Vous découvrez les intégrations Slack ?

Consultez notre guide [Premiers pas](#) pour vous familiariser avec les types d'intégration les plus courants et pour trouver des conseils dont vous tiendrez compte en créant la vôtre. Si vous le souhaitez, [register as a developer](#) (inscrivez-vous en tant que développeur) pour nous faire connaître le projet sur lequel vous travaillez et recevoir les mises à jour futures de nos API.

Instructions d'installation

Nous vous guiderons à travers les étapes nécessaires à la configuration d'un webhook entrant afin que vous puissiez commencer à envoyer des données vers Slack.

fermer

URL du webhook

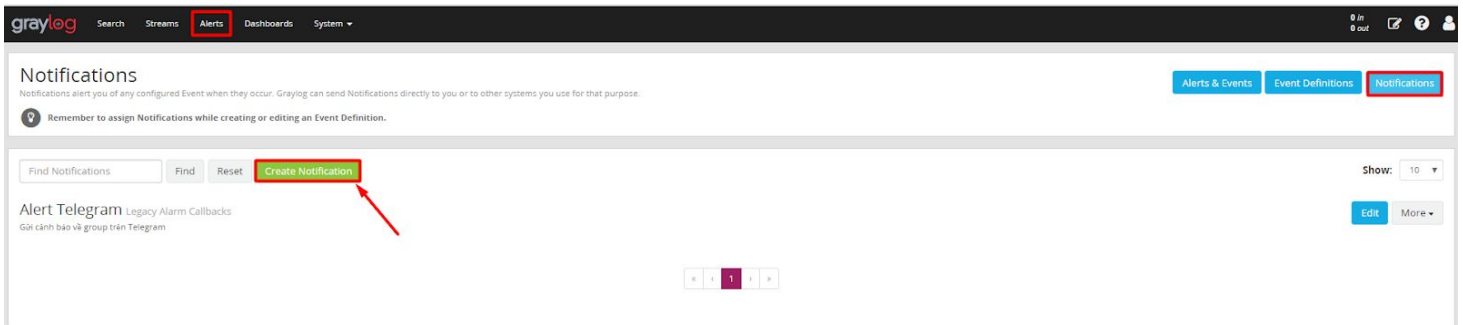
<https://hooks.slack.com/services/TRT0DTR6/BUK1P43K3/g5UoeN8kv99Q1k0ETZ4vLq2c>

Envoyer des messages

Vous avez deux possibilités pour envoyer les données à l'URL du webhook ci-dessus :

- Envoyer une chaîne JSON comme paramètre `payload` dans une requête POST
- Envoyer une chaîne JSON comme corps d'une requête POST

- **Tiếp đến, trên Web Interface của graylog-server vào Alerts -> Notification -> Create Notification**



- **Chọn các trường phù hợp với cảnh báo Slacks**

New Notification

Alerts & Events

Event Definitions

Notifications

Graylog's new Alerting system let you define more flexible and powerful rules. [Learn more in the documentation](#)

Title

Slack Alert

Title to identify this Notification.

Description (Optional)

Gửi cảnh báo về Slack

Longer description for this Notification.

Notification Type

Legacy Alarm Callbacks

Choose the type of Notification to create.

Choose Legacy Notification

Legacy Slack Alarm Callback

Select a Legacy Notification to use on this Event Definition.

Legacy alarm callbacks are deprecated. Please switch to the new notification types as soon as possible!

- Nhập URL Webhooks và nhập channel mà cảnh báo sẽ gửi về

Color to use for Slack custom message:

Custom Message (optional)

#####

Alert Description: \${check_result.resultDescription}

Date: \${check_result.triggeredAt}

Stream ID: \${stream.id}

Stream title: \${stream.title}

Stream description: \${stream.description}

Alert Condition Title: \${alert_condition.title}

\${if stream_url}Stream URL: \${stream_url}\${end}

Triggered condition: \${check_result.triggeredCondition}

Custom message to be appended below the alert title. The following properties are available for template building: "stream", "check_result", "stream_url", "alert_condition", "backlog", "backlog_size". See <http://docs.graylog.org/erv2.3/pages/streams/alerts.html#email-alert-notification> for more details.

Webhook URL

https://hooks.slack.com/services/TRT0DTR6/BUK1P43K3/oSUoeN8kw99QikD0TZ4vLqZo

Slack "Incoming Webhook" URL

Channel

#graylog

Name of Slack #channel or @user for a direct message.

User name (optional)

Graylog

- Nhập vào URL Web Interface của graylog và bấm vào **Execute Test Notification** để gửi thử 1 cảnh báo mẫu về channel :

User name (optional)

User name of the sender in Slack.

Backlog items

Number of backlog item descriptions to attach

☐ **Notify Channel**
Notify all users in channel by adding @channel to the message.

☒ **Link names**
Find and link channel names and user names

Icon URL (optional)

Image to use as the icon for this message

Icon Emoji (optional)

Emoji to use as the icon for this message (overrides icon URL)

Graylog URL (optional)

URL to your Graylog web interface. Used to build links in alarm notification.

Proxy (optional)

Please insert the proxy information in the following format: <ProxyAddress><Port>

Test Notification (Optional)

- Nếu nhận được cảnh báo như này có nghĩa là đã thành công :



Graylog
APPLI
21 h 48

Alert for Graylog stream *Missing stream*:

Notification test message triggered from user <admin>

Custom Message:

#####

Alert Description: Notification test message triggered from user <admin>

Date: 2020-03-04T14:48:21.361Z

Stream ID: 5e5fbfb59ace6608c02a8132

Stream title: Missing stream

[En afficher plus](#)

- Sau khi nhận cảnh báo thành công, bấm **Create** để tạo và lưu lại cấu hình.

Graylog URL (optional)

URL to your Graylog web interface. Used to build links in alarm notification.

Proxy (optional)

Please insert the proxy information in the following format: <ProxyAddress><Port>

Test Notification (Optional)

Execute Test Notification

Success: Notification was executed successfully.

Execute this Notification with a test Alert.

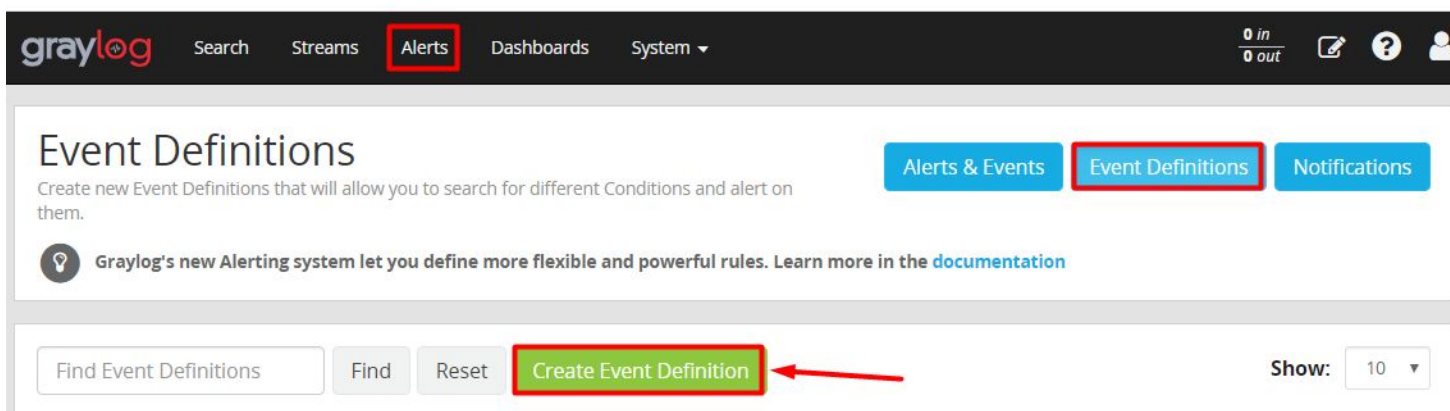
Create Cancel

Note: Có thể tham khảo thêm về cách tạo cảnh báo Slack [tại đây](#).

3.2 Cấu hình gửi cảnh báo

Bước 1: Cấu hình Event cảnh báo

- Trên Web Interface của graylog-server, vào mục Alerts chọn tab Event Definitions và chọn Create Event Definition để tạo 1 cảnh báo về các sự kiện.



- Đặt tên cho cảnh báo và mô tả ngắn về cảnh báo, chọn mức cảnh báo là Normal và Next để tiếp tục .

Event Details

Title
SSH Accepted

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

Description (Optional)
Gửi cảnh báo khi có SSH thành công

Longer description for this Event Definition.

Priority
Normal

Choose the priority for Events created from this Definition.

Previous Next

- Điền các mục cần thiết như sau và chọn Next để tiếp tục :

Event Condition

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
Action:Accepted

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 `$lookupparameter` syntax.

Streams (Optional)
All messages

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

Search within the last
1 minutes

Execute search every
1 minutes

Create Events for Definition if...
☒ Filter has results
☐ Aggregation of results reaches a threshold

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

Could not find any messages with the current search criteria.

Previous Next

Note:

- Chọn Condition Type là Filter & Aggregation
- Ở mục Search Query nhập vào truy vấn để lọc ra những bản tin log phù hợp với tiêu chí cảnh báo
- Chọn Streams là All Messages để search toàn bộ message (ta có thể tạo 1 streams để lọc 1 bản tin riêng)
- Đặt thời gian cách mỗi lần tìm kiếm là 1 phút và tìm trong vòng 1 phút cuối cùng.

- Tiếp đến là **Event Fields**, là 1 trường bổ sung thông tin về cảnh báo và thêm ngữ cảnh khi cảnh báo nhưng là 1 trường không bắt buộc nên ta có thể bỏ qua.

- Mục tiếp theo là mục **Notification**, click chọn **Add Notification** và chọn các cảnh báo về Telegram, Email, Slack đã tạo trước đó.

- Đầu tiên ta add cảnh báo về Telegram

- Chọn **Done** để xác nhận.

Event Details
Condition
Fields
Notifications
Summary

Add Notification

Choose Notification

Alert Telegram X ▼

Select a Notification to use on Alerts of this kind or create a new Notification that you can later use in other Alerts.

Done

Cancel

Previous

Next

- Tương tự như add cảnh báo telegram, ta add các cảnh báo của Email và Slack. Chọn Next để chuyển sang bước tiếp.

Event Details
Condition
Fields
Notifications
Summary

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
Alert Telegram	Legacy Alarm Callbacks	Remove from Event
Email Alert	Email Notification	Remove from Event
Slack Alert	Legacy Alarm Callbacks	Remove from Event

Add Notification

Previous

Next

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

☒ 1

Number of messages to be included in Notifications.

- Tại bước này cung cấp 1 bản tóm tắt về định nghĩa cảnh báo vừa tạo. Chọn Done để hoàn tất cài đặt Alert.

Event Details

Filter & Aggregation

Fields

Notifications

Summary

Event Summary

Details

Title
SSH Accepted

Description
Gửi cảnh báo khi có SSH thành công

Priority
Normal

Fields

No Fields configured for Events based on this Definition.

Filter & Aggregation

Type
Filter

Search Query
Action:Accepted

Streams
All messages

Search within
1 minutes

Execute search every
1 minutes

Notifications

Settings
Grace Period is disabled
Notifications will include 1 messages

Alert Telegram
Legacy Alarm Callbacks

[Less details](#)

Description	Gửi cảnh báo về group trên Telegram
Message	\${stream_uri}: \${stream.title} <code>\${foreach backlog message} \${message.message} </code>
Chat IDs	-407238775
Parse Mode	HTML
Bot Token	1129852247:AAEiKCoQDHau9iYyo2jm14K3-wzC6Pcv3Y
Graylog URL	http://103.101.161.205:9000/
Proxy	

Cancel

Done

Bước 2: Kiểm tra cấu hình cảnh báo.

- Tiến hành ssh vào client c7srv01 và U16SRV02 để kiểm tra xem có cảnh báo gửi về hay không.

Tiến hành ssh vào client c7srv01

```
[root@graylogall ~]# ssh root@192.168.70.93
root@192.168.70.93's password:
Last login: Fri Mar 6 08:01:08 2020 from 192.168.70.84
```

Tiến hành ssh vào U16SRV02

```
root@192.168.80.210's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '18.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Mar 6 08:09:15 2020 from 192.168.80.94
```

- Kiểm tra kết quả cảnh báo

1. Trong telegram

Ta thấy rằng đã có đủ cảnh báo của 2 client.

All messages: SSH Accepted

```
Hostname:c7srv01 IP:192.168.70.84 User:root
```

```
Mar  6 08:03:30 c7srv01 sshd[9147]: Accepted password for  
root from 192.168.70.84 port 59898 ssh2
```

All messages: SSH Accepted

```
Hostname:U16SRV02 IP:192.168.80.94 User:root
```

```
Mar  6 08:14:27 U16SRV02 sshd[3873]: Accepted password for  
root from 192.168.80.94 port 35102 ssh2
```

2. Kiểm tra Email

Ta thấy email cũng có đủ cả cảnh báo từ 2 client.



hungnvnhanhoa@gmail.com

tới tôi ▾



Tiếng Anh ▾



Tiếng Việt ▾

[Dịch thư](#)

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

Title: SSH Accepted

Description: Gửi cảnh báo khi có SSH thành công

Type: aggregation-v1

--- [Event] -----

Timestamp: 2020-03-06T01:03:39.457Z

Message: SSH Accepted

Source: graylogall

Key:

Priority: 2

Alert: true

Timestamp Processing: 2020-03-06T01:03:39.457Z

Timerange Start:

Timerange End:

Fields:

--- [Backlog] -----

Last messages accounting for this alert:

++

Hostname:c7srv01 IP:192.168.70.84 User:root

Mar 6 08:03:30 c7srv01 sshd[9147]: Accepted password for root from 192.168.70.84 port 59898 ssh2



hungnvnhanhoa@gmail.com

tới tôi ▾



Tiếng Anh ▾



Tiếng Việt ▾

[Dịch thư](#)

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

Title: SSH Accepted

Description: Gửi cảnh báo khi có SSH thành công

Type: aggregation-v1

--- [Event] -----

Timestamp: 2020-03-06T01:14:29.115Z

Message: SSH Accepted

Source: graylogall

Key:

Priority: 2

Alert: true

Timestamp Processing: 2020-03-06T01:14:29.115Z

Timerange Start:

Timerange End:

Fields:

--- [Backlog] -----

Last messages accounting for this alert:

++

Hostname:U16SRV02 IP:192.168.80.94 User:root

Mar 6 08:14:27 U16SRV02 sshd[3873]: Accepted password for root from 192.168.80.94 port 35102 ssh2

3. Kiểm tra cảnh báo từ Slack

Alert for Graylog stream **All messages**:

SSH Accepted

Custom Message:

#####

Alert Description: SSH Accepted

Date: 2020-03-06T01:05:41.752Z

Stream ID: 00000000000000000000000001

Stream title: All messages

Stream description: Stream containing all messages

Alert Condition Title: SSH Accepted

Stream URL:

<http://103.101.161.205:9000/streams/00000000000000000000000001/messages?q=%2A&rangetype=relative&relative=3600>

Triggered condition: 5e5f0ae59ace6677c8344e14:aggregation-v1={SSH Accepted},
stream:={00000000000000000000000001: "All messages"}

#####

Last messages accounting for this alert:

source: c7srv01 | message: Mar 6 08:03:30 c7srv01 sshd[9147]: Accepted password

Alert for Graylog stream **All messages**:

SSH Accepted

Custom Message:

#####

Alert Description: SSH Accepted

Date: 2020-03-06T01:17:10.995Z

Stream ID: 00000000000000000000000001

Stream title: All messages

Stream description: Stream containing all messages

Alert Condition Title: SSH Accepted

Stream URL:

<http://103.101.161.205:9000/streams/00000000000000000000000001/messages?q=%2A&rangetype=relative&relative=3600>

Triggered condition: 5e5f0ae59ace6677c8344e14:aggregation-v1={SSH Accepted},
stream:={00000000000000000000000001: "All messages"}

#####

Last messages accounting for this alert:

source: U16SRV02 | message: Mar 6 08:14:27 U16SRV02 sshd[3873]: Accepted

Ta thấy đã có đủ cảnh báo gửi về, như vậy là đã thành công.

