

对比过ELK、商业日志工具Splunk和Graylog，后面选择了Graylog。Graylog简单说就是一个开源的日志聚合、分析、审计、展现和预警工具。

1. Graylog优点。

- 零开发：从收集->存储->分析->呈现完整流程。
- 部署维护简单：一体化解决方案，不像ELK三个独立系统集成。
- 多日志源接入：syslog、Filebeat、Log4j、Logstash等。
- 多协议接入：UDP、TCP、HTTP、AMQP。
- 自定义面板：提供曲线图、饼状图、世界地图等丰富的图形列表。
- 全文搜索：支持按语法进行过滤搜索全部日志。
- 支持报警：具有报警功能的日志分析平台。
- 权限管理：灵活的权限分配和管理。
- 支持集群：可以根据应用扩展平台性能。

2. Graylog架构设计，支持集群。

- GrayLog：提供 GrayLog对外接口，CPU 密集。
- Elasticsearch：日志文件的持久化存储和检索，IO 密集。
- MongoDB：存储一些 GrayLog 的配置信息。
- PrometheusAlert: 提供日志告警服务

3. 安装Graylog3

- 安装依赖包

```
# yum install epel-release -y
# yum install pwgen -y
```

- 安装mongodb

```
# vim /etc/yum.repos.d/mongodb-org-3.6.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

# 安装
# yum install -y mongodb-org

# 启动
# systemctl enable mongod
# systemctl start mongod
```

- 安装Elasticsearch

```

# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
# graylog3.0 使用的elasticsearch不低于5.6.13版本, 我这里用的最新版6.x
# vim /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

# 如果官网下载较慢也可以使用华为的镜像源
wget
https://mirrors.huaweicloud.com/elasticsearch/6.5.0/elasticsearch-
6.5.0.rpm

# 安装
# yum install java
# yum install elasticsearch

#修改配置, 设置JAVA_HOME
#vim /etc/sysconfig/elasticsearch
#-----
#JAVA_HOME=/usr/share/elasticsearch/jdk # 填上自己的java_home路径
#-----

# 启动
# systemctl enable elasticsearch
# systemctl start elasticsearch

# 查看
# curl -XGET 'http://localhost:9200/'

```

o 安装Graylog3

```

$ rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-3.0-
repository_latest.rpm
$ yum install graylog-server -y

```

修改配置, password_secret和root_password_sha2是必须的, 不设置则无法启动, 设置方法如下:

```

# 修改配置
vim /etc/graylog/server/server.conf
-----
-----

```

```
# password_secret可以通过命令: pwgen -N 1 -s 96 来随机生成, 下面就是我随机生成的
password_secret =
6Z06fZHU2DwuOf9X8fhnvphCd3OM7oqwLEcRRcejvvpieSvVtwu08yHYHIKDi56bAxRvtC
OZ3xKKiBqyt00XYCgVa0oETB0L

# admin用户密码生成命令: echo -n yourpassword | sha256sum
# 生成后, 请记住你的 YourPassword
root_password_sha2 =
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

# admin用户邮箱
root_email = "root@example.com"

# 时区
root_timezone = Asia/Shanghai

# elasticsearch 相关配置
elasticsearch_hosts = http://127.0.0.1:9200
elasticsearch_shards =1
elasticsearch_replicas = 0

# mongodb 连接配置, 这里直接本机起的mongodb, 没有设置验证
mongodb_uri = mongodb://localhost/graylog

# 电子邮件smtp, 设置为自己的邮箱smtp服务
transport_email_enabled = true
transport_email_hostname = smtp.exmail.qq.com
transport_email_port = 465
transport_email_use_auth = true
transport_email_use_tls = false
transport_email_use_ssl = true
transport_email_auth_username = root@example.com
transport_email_auth_password = 123456
transport_email_subject_prefix = [graylog]
transport_email_from_email = root@example.com
transport_email_web_interface_url = http://graylog.example.com

# 网络访问相关, 重要, graylog3比2.x版本简洁了很多网络配置, 只需配置
http_bind_address即可。
http_bind_address = 0.0.0.0:9000

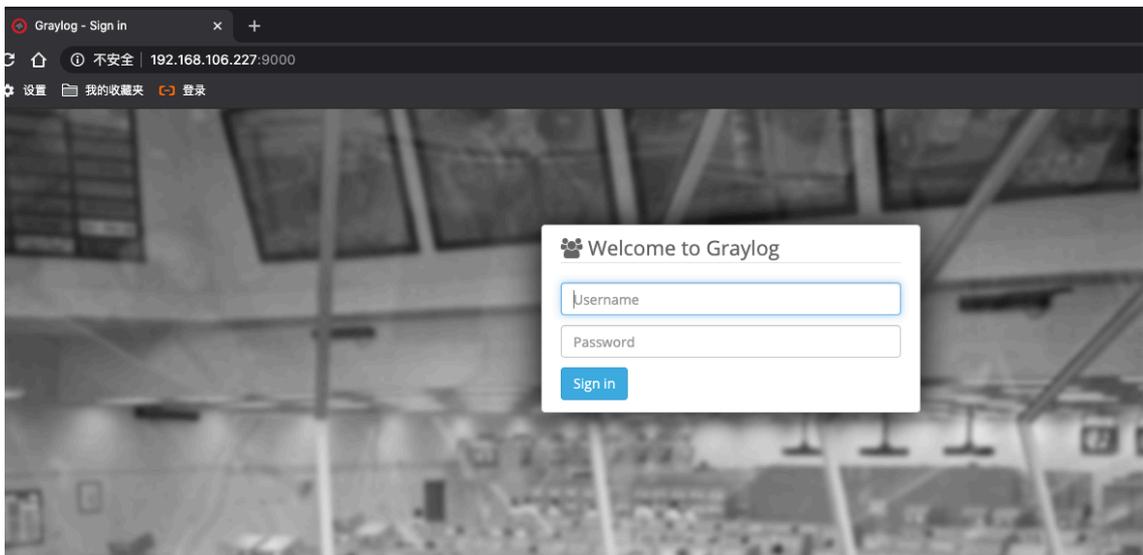
# 配置外网地址, 我这里用了域名+nginx做反向代理, 所以外网地址如下。没有的话就直接就
用外网ip+port, 如: http://外网ip:9000/
http_publish_uri = http://graylog.example.com/

# http_external_uri = http://graylog.example.com/ 单节点的话, 此配置不需要
配置, 默认使用http_publish_uri
```

```
-----  
-----  
# 启动需要手动设置Java路径  
vim /etc/sysconfig/graylog-server  
-----  
-----  
JAVA=/usr/local/jdk1.8.0_191/bin/java  
-----  
-----  
  
# 启动服务  
$ systemctl enable graylog-server  
$ systemctl start graylog-server
```

- o 访问web页面

按照上面配置，直接配置成外网ip地址，那么直接访问 <http://外网ip:9000>，就可以进入web登陆页面



输入用户密码登陆

admin

123456

4. 安装Graylog Sidecar (Graylog Collector Sidecar)

Graylog Sidecar是一个轻量级配置管理系统，适用于不同的日志收集器，也称为后端。Graylog节点充当包含日志收集器配置的集中式集线器。在支持的消息生成设备/主机上，Sidecar可以作为服务（Windows主机）或守护程序（Linux主机）运行。进行在不同机器上进行日志的采集并发送到graylog server

在graylog3.0版本以前，称为Graylog Collector Sidecar，在3.0中改为了Graylog Sidecar，在官方文档中有详细安装指导：

。这里也参考进行安装。版本对照表如下，首先去github上下载相应的rpm安装包。

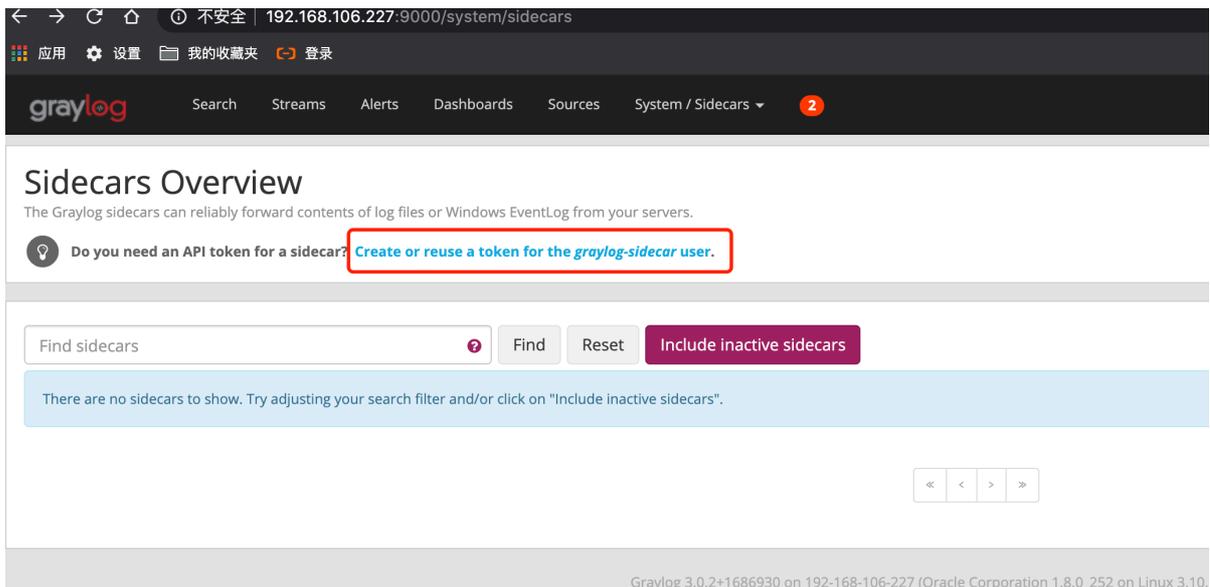
```
# wget https://github.com/Graylog2/collector-
sidecar/releases/download/1.0.2/graylog-sidecar-1.0.2-1.x86_64.rpm
# rpm -i graylog-sidecar-1.0.2-1.x86_64.rpm
# 修改配置
# vim /etc/graylog/sidecar/sidecar.yml

-----
--
server_url: "http://127.0.0.1:9000/api/"      # api的外网地址
# api token 必要的, 不然启动不了, token需要在web界面上进行手动创建
server_api_token: "1jq26cssvc6rj4qac4bt9oeeh0p4vt5u5ka19joc11g9mdi4og3n"
node_name: "graylog-server-localhost"     # 自定义节点名称
update_interval: 10
send_status: true

-----
--

# 安装系统服务
# graylog-sidecar -service install
# systemctl start graylog-sidecar
# systemctl enable graylog-sidecar
```

创建token方法如下:

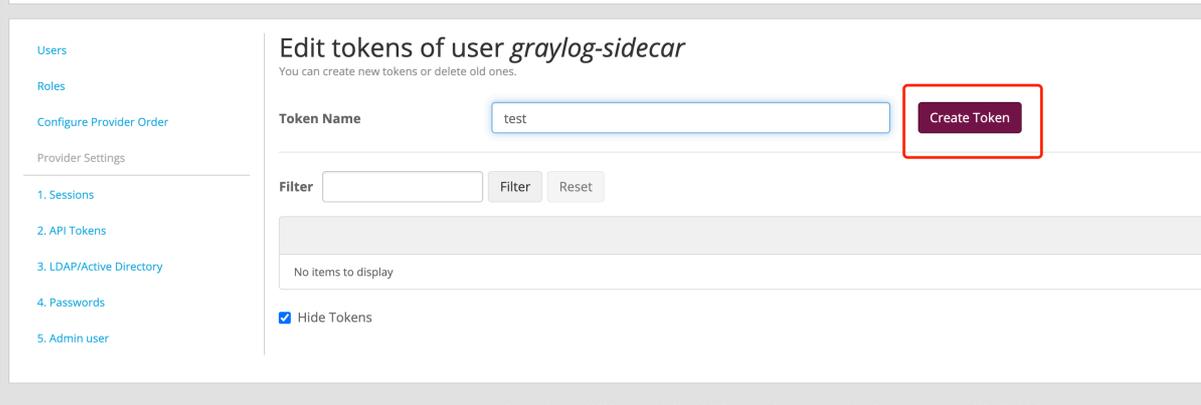


The screenshot shows the Graylog web interface. The browser address bar displays "192.168.106.227:9000/system/sidecars". The navigation menu includes "Search", "Streams", "Alerts", "Dashboards", "Sources", and "System / Sidecars". The main heading is "Sidecars Overview". Below the heading, there is a message: "Do you need an API token for a sidecar?" with a link "Create or reuse a token for the graylog-sidecar user." highlighted by a red box. Below this, there is a search bar with the text "Find sidecars" and buttons for "Find", "Reset", and "Include inactive sidecars". A message below the search bar states: "There are no sidecars to show. Try adjusting your search filter and/or click on 'Include inactive sidecars'." At the bottom of the page, the footer text reads: "Graylog 3.0.2+1686930 on 192-168-106-227 (Oracle Corporation 1.8.0_252 on Linux 3.10.)"

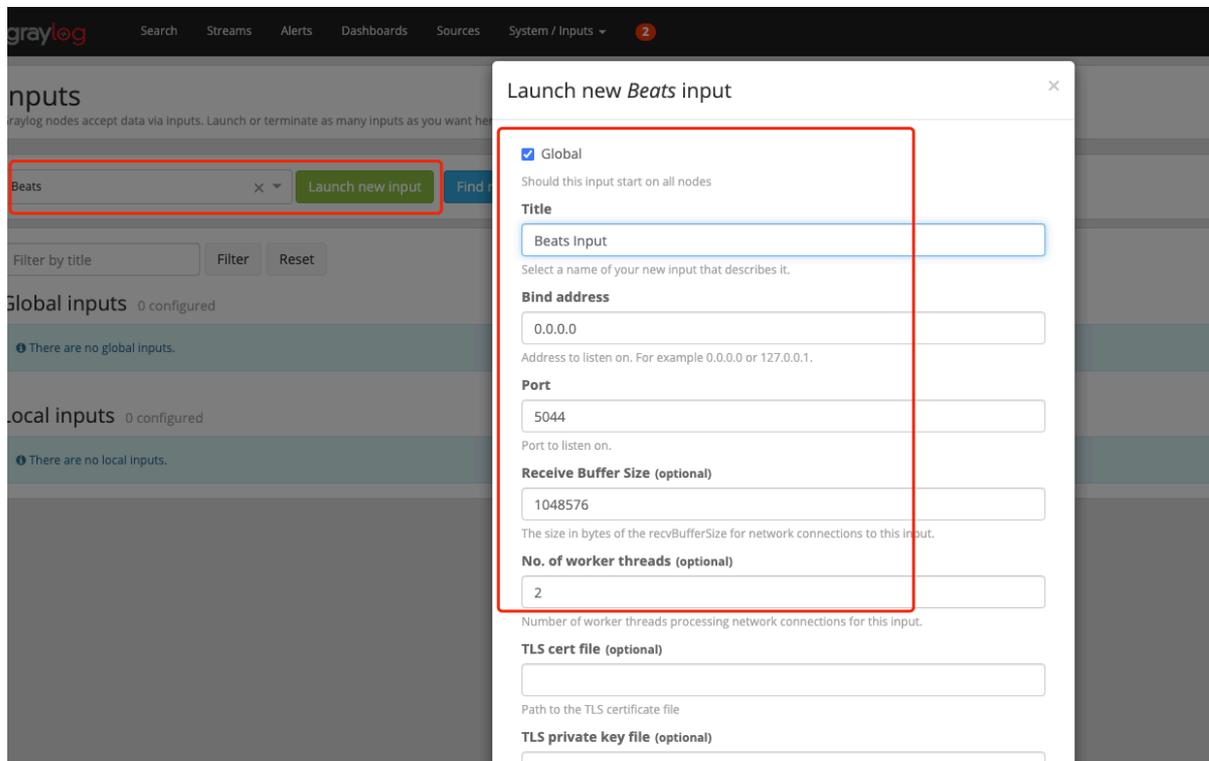
Authentication Management

Configure Graylog's authentication providers and manage the active users of this Graylog cluster.

 Read more authentication in the [documentation](#).



ok, 到此就可以启动graylog-sidecar了。启动后, 在web界面上就可以看到有一个节点了, 然后下面记录怎么手动配置这个节点的日志采集。首先需要创建一个beats的input, 因为我要要用filebeat进行日志采集。



然后就需要定义sidecar的filebeat配置, 用这个配置来启动filebeat进行日志采集, 并输入到上面定义的beats input。但是graylog3.0中, graylog sidecar的linux版本不包含filebeat(3.0版本之前是默认包含filebeat的), 需要自己手动下载安装filebeat, 安装非常简单, 通过官方下载页面, 直接下载rpm包进行安装就行: [官方下载地址](#)

PS: 我这里是演示的用filebeat进行日志采集, 如果用nxlog进行采集, 同样的需要安装nxlog程序。

```
# wget https://mirrors.huaweicloud.com/filebeat/6.6.0/filebeat-6.6.0-x86_64.rpm
# rpm -i filebeat-6.6.0-x86_64.rpm
```

ok, 就这样就ok啦, 然后下面在web界面上进行配置

graylog Search Streams Alerts Dashboards Sources System / Sidecars 1 In 0 / Out 0 msg/s Help Administrator

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.](#)

Overview Administration **Configuration**

Find sidecars Find Reset Include inactive sidecars Show: 50

Name	Status	Operating System	Last Seen	Node Id	Sidecar Version	Actions
graylog-server-localhost	▶ Running	Linux	a few seconds ago	51201c8b-2029-49df-b790-ddf6cd7c719	1.0.2	Manage sidecar Show messages

Log Collectors 4 total

Manage Log Collectors that you can configure and supervise through Graylog Sidecar and Graylog Web interface.

Find collectors Find Reset Show: 10 [Create Log Collector](#)

Name	Operating System	Actions
filebeat	Linux	Edit More actions
nxlog	Linux	Edit More actions
nxlog	Windows	Edit More actions
winlogbeat	Windows	Edit More actions

这里我以采集本机上graylog-server的日志为例子，自定义变量中定义beats input服务的ip和端口，使得sidecar采集器能将数据输入指定input，并可以在所有配置中直接复用。

Edit Variable `${user.graylog_beats_input}`

Name

Type a name for this variable

Description (Optional)

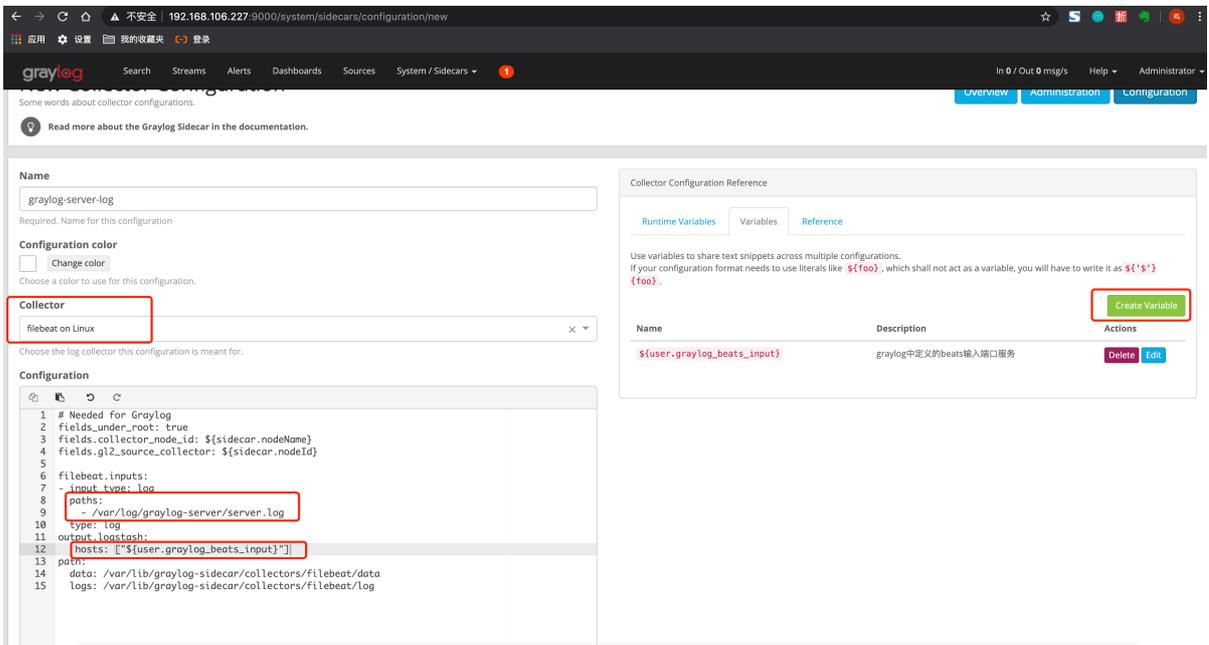
Type a description for this variable

Content

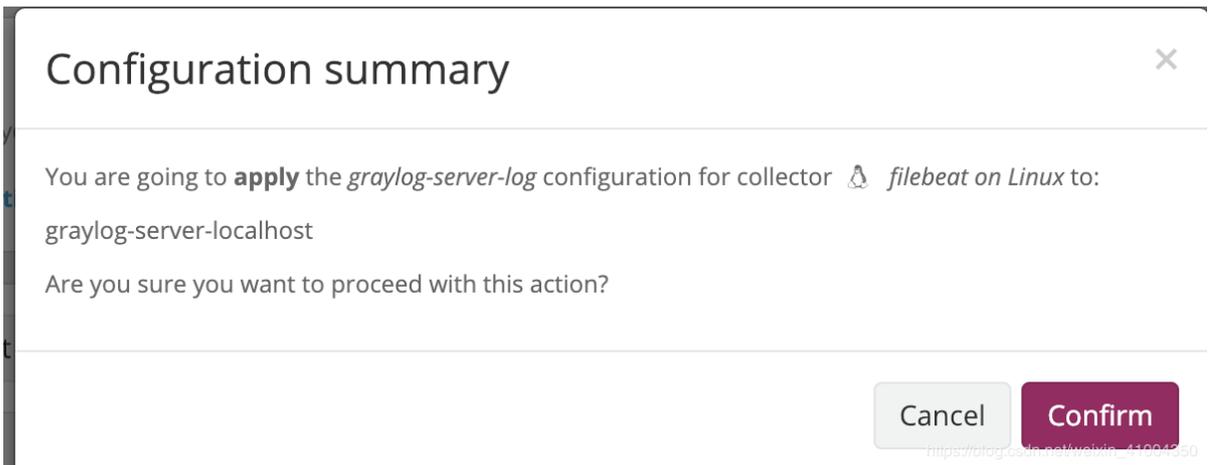
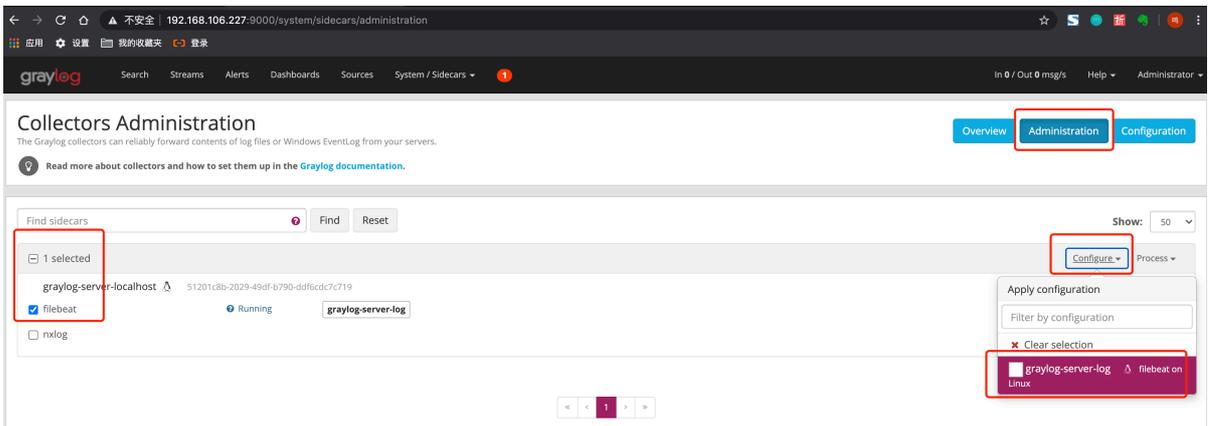
Write your variable content

Cancel

Save



配置创建完成后，需要将配置与指定sidecar进行联系，然后sidecar就能以执行配置启动filebeat进行日志采集。如图：



然后就能在web界面上，看到采集到的graylog-server的日志

The screenshot shows the Graylog web interface. At the top, there's a search bar with a dropdown menu set to 'Search in the last 5 minutes'. Below the search bar, there's a search result section with a histogram and a list of messages. The histogram shows a single bar at 10:06. The messages list shows several entries with timestamps and source IP addresses.

5. 配置接入syslog

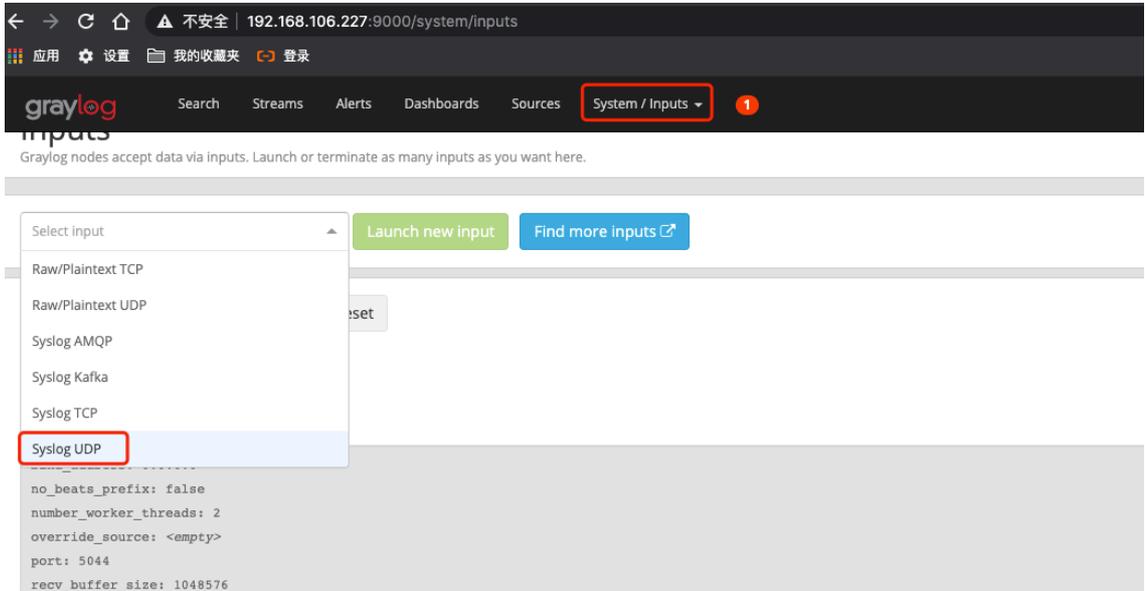
- 修改graylog配置

```
# touch /etc/rsyslog.d/greylog.conf #创建rsyslog额外配置文件
# cat << EOF > /etc/rsyslog.d/greylog.conf #编辑配置文件
> *.* @192.168.106.227:1515;RSYSLOG_SyslogProtocol23Format #*.*
代表linux中所有模块所有级别的日志, @代表使用udp协议, @@代表使用tcp协议,
192.168.106.227:1515 greylog主机的IP和收集端口
> EOF #RSYSLOG_SyslogProtocol23Format
代表syslog协议格式模板
```

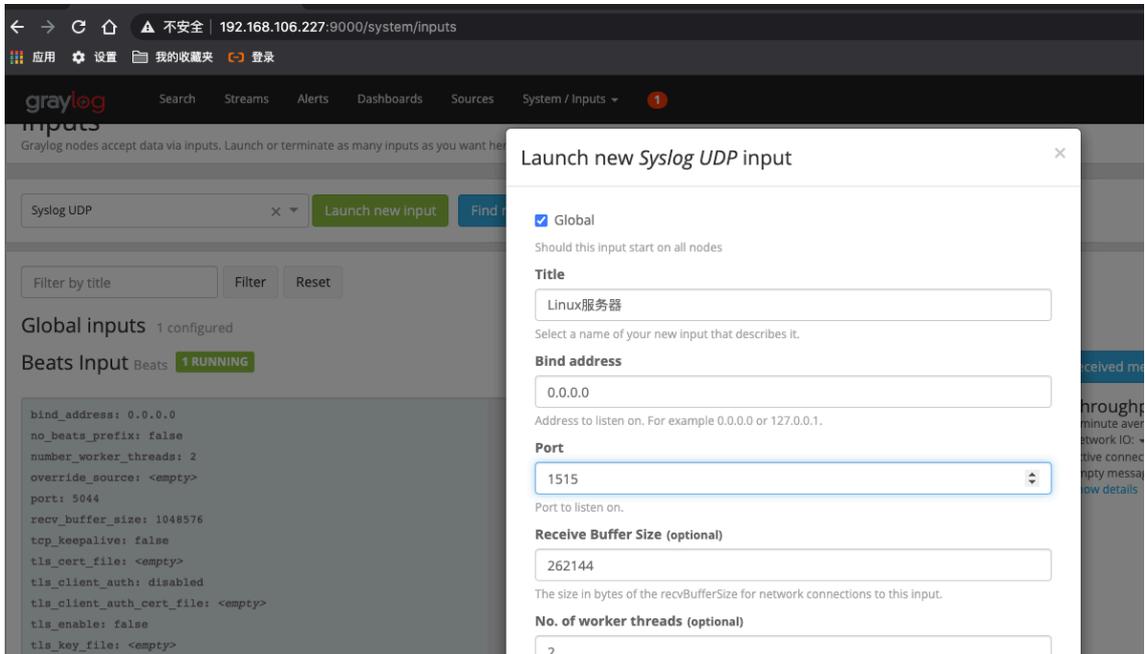
- 配置完成后, 重启rsyslog服务

```
# systemctl restart rsyslog
```

- 然后在到graylog上进行配置, 在system->input中, 添加一个新的input,按照如下进行配置, 选择Syslog UDP



点击launch new input, 然后按照如下进行配置



说明:

1、port 写1515

2、bind address保持0.0.0.0 默认

完成添加后, 点击“start input”启动

- 然后我们在一台linux主机上进行测试, 使用简单测试用命令, 检查greylog是否能够收到

```
#如果rsyslog没有安装的话先装一下
# yum install rsyslog
# systemctl restart rsyslog
# systemctl enable rsyslog
# logger -p mail.info "hello"!
```

- 确认可以收到

Search result
Found 1 messages in 115 ms, searched in 1 index.
Results retrieved at 2020-06-17 10:47:20.

Histogram
Year, Quarter, Month, Week, Day, Hour, Minute

Messages

Timestamp	source
2020-06-17 10:46:25.613	192-168-106-227

Received by
Linux 服务器 on P 22f012ae / 192-168-106-227

Stored in index
graylog_0

Routed into streams
• All messages

message
hello!

application_name
zoo1

facility
mail

level
6

source
192-168-106-227

timestamp
2020-06-17 10:46:25.613 +08:00

6. 配置告警

这里接入的也是PrometheusAlert

- o PrometheusAlert添加配置

```
# cd /opt/app/PrometheusAlert/conf
# vim app.conf
#链接到告警平台地址
GraylogAlerturl=http://192.168.106.227:9000
```

- o 添加新的alert

Manage alert notifications

Notifications let you be aware of changes in your alert conditions status any time. Graylog can send notifications directly to you or to other systems you use for that purpose.

Remember to assign the notifications to use in the alert conditions page.

Notifications

These are all configured alert notifications.

There are no configured notifications.

Notification

Define the notification that will be triggered from the alert conditions in a stream.

Notify on stream
All messages

Notification type
HTTP Alarm Callback

Add alert notification

Editing alert configuration



Title

URL

The URL to POST to when an alert is triggered

Cancel

Save

接口说明

特别说明：graylog3接口针对 graylog版本 $\geq 3.1.x$

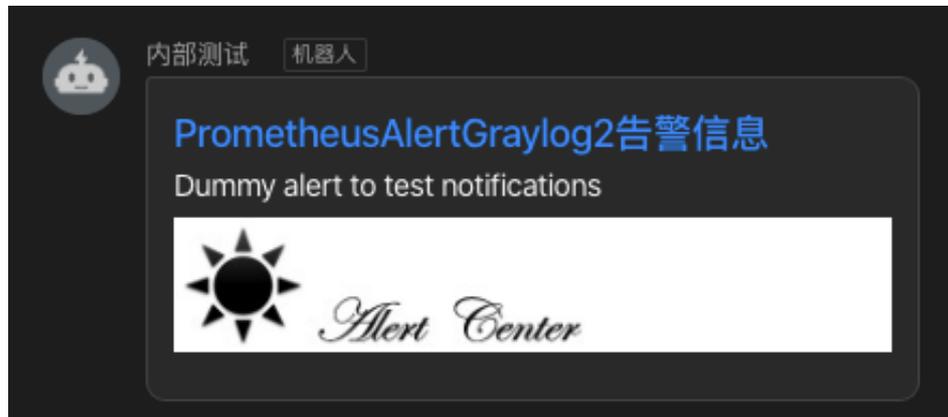
/graylog3/dingding	处理Graylog3告警消息转发到钉钉接口，可选参数(ddurl)
/graylog3/weixin	处理Graylog3告警消息转发到微信接口，可选参数(wxurl)
/graylog3/feishu	处理Graylog3告警消息转发到飞书接口，可选参数(fsurl)
/graylog3/txdx	处理Graylog3告警消息转发到腾讯云短信接口，可选参数(phone)
/graylog3/txdh	处理Graylog3告警消息转发到腾讯云电话接口，可选参数(phone)
/graylog3/hwdx	处理Graylog3告警消息转发到华为云短信接口，可选参数(phone)
/graylog3/alydx	处理Graylog3告警消息转发到阿里云短信接口，可选参数(phone)
/graylog3/alydh	处理Graylog3告警消息转发到阿里云电话接口，可选参数(phone)
/graylog3/rlydh	处理Graylog3告警消息转发到容联云电话接口，可选参数(phone)

关于接口说明：graylog的所有接口均支持传参,如直接使用接口，未在接口后加入参数，默认会优先使用配置文件中的参数作为告警渠道的配置。如果接口中加入了参数，将默认使用url中的参数作为告警渠道的配置。如下：

```
/graylog3/dingding?ddurl=https://oapi.dingtalk.com/robot/send?
access_token=xxxxx
/graylog3/weixin?wxurl=https://qyapi.weixin.qq.com/cgi-
bin/webhook/send?key=xxxxx
/graylog3/feishu?fsurl=https://open.feishu.cn/open-
apis/bot/hook/xxxxxxxxx
/graylog3/txdx?phone=15395105573
/graylog3/txdh?phone=15395105573
/graylog3/hwdx?phone=15395105573
/graylog3/alydx?phone=15395105573
/graylog3/alydh?phone=15395105573
/graylog3/rlydh?phone=15395105573
```

配置完成后,点击 Test 测试下是否能够正常接收告警消息即可

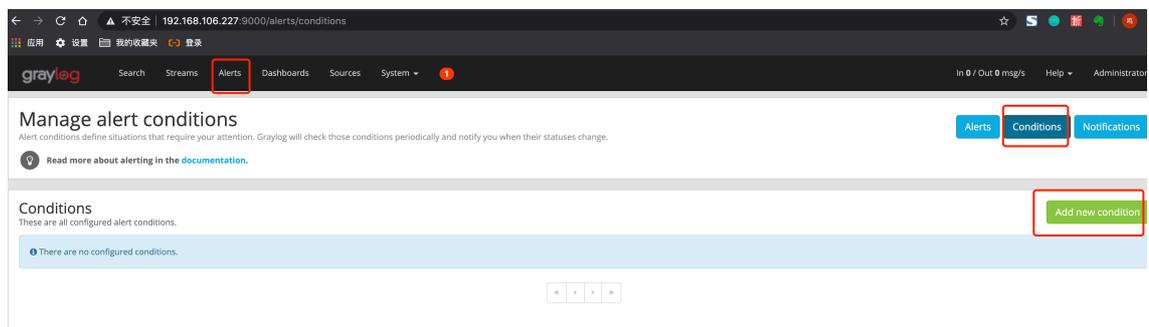
最终告警效果:



注意：由于这里graylog版本太旧，只能用graylog2的接口

实例测试

配置告警条件为包含OutOfMemoryError内容的就报警



New alert condition

Define an alert condition and configure the way Graylog will notify you when that condition is satisfied.

Are the default conditions not flexible enough? You can write your own! Read more about alerting in the [documentation](#).

Condition

Define the condition to evaluate when triggering a new alert.

Alert on stream

All messages

Select the stream that the condition will use to trigger alerts.

Condition type

Field Content Alert Condition

Select the condition type that will be used.

Add alert condition

Create new Field Content Alert Condition



Field Content Alert Condition description

This condition is triggered when the content of messages is equal to a defined value.

Title

The alert condition title

Field

Field name that should be checked

Value

Value that the field should be checked against

Grace Period

Number of minutes to wait after an alert is resolved, to trigger another alert

Message Backlog

The number of messages to be included in alert notifications

Search Query (optional)

Query string that should be used to filter messages in the stream

Repeat notifications (optional)

Check this box to send notifications every time the alert condition is evaluated and satisfied regardless of its state.

Cancel

Save

Field: 要检查的字段, 这里写message

Value: 要查找的内容, 这里写OutOfMemoryError

Message Backlog: 大于多少个值这里设置为3, 也就是出现三个就报警

o 制造日志测试

```
# logger -p mail.info "OutOfMemoryError"!
# logger -p mail.info "OutOfMemoryError"!
# logger -p mail.info "OutOfMemoryError"!
```

结果如下:

 内部测试 机器人

PrometheusAlertGraylog2告警信息

Stream received messages matching
message:"OutOfMemoryError" (Current grace time: 0
minutes)

告警索引: graylog_0
开始时间: 2020-06-17 12:32:36.959
告警主机: 192.168.106.227:0
OutOfMemoryError!

