



MONITORANDO LOGS COM
[GRAYLOG]



\$WHOAMI

Bezaleel(Beza)

Onx Solutions – Monitoração e DevOps

Certification LPIC

Zabbix Certifield Specialist

O QUE É O GRAYLOG



Ferramenta que permite o
fácil gerenciamento de logs
de dados estruturados e
não estruturados

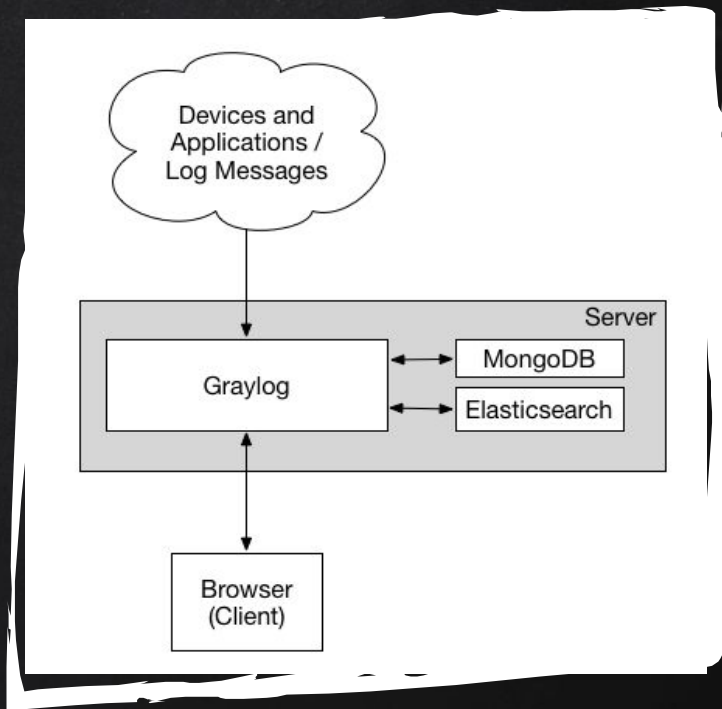


INSTALAÇÃO

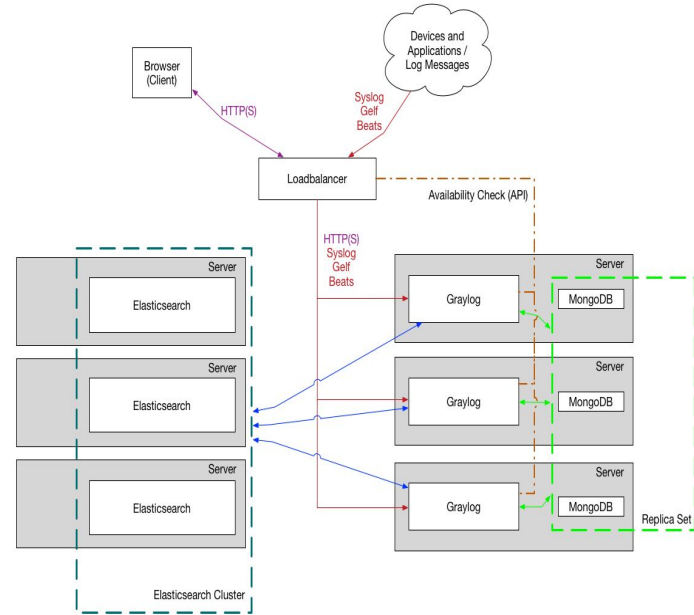
- ✕ Debian / Ubuntu (deb package)
- ✕ RedHat / Centos (RPM package)
- ✕ Virtual Machine (OVA/Vagrant)
- ✕ Docker image && docker compose
- ✕ Config management (Chef / Puppet / Ansible)

ARQUITETURA

BÁSICO



MULTI-NODE





COMPONENTES

MongoDB

Usado para armazenar metadata(usuário, configurações, streams, dashboards, extractores etc).

Elasticsearch

Armazena todos os logs/mensagens e pesquisa de texto, exige bastante memória e I/O

GrayLog Server

Funciona como um worker que recebe, processa as mensagens e comunica com todos os outros componentes, exige bastante CPU.



BACKUP

- ✗ MongoDB:
 - DB dump
- ✗ Elasticsearch:
 - Repositório , Snapshot e Restore
 - *Curator



FINALIDADE DO LOG

Debug

BI

Auditoria

Monitorar



COMO ACESSAR OS LOGS?

Aplicação
que escreve
em arquivo

Acesso
remoto

\$ tail,grep,
awk



COMO COLETAR

Syslog (TCP, UDP, AMQP,
Kafka)

GELF (TCP, UDP, AMQP,
Kafka, HTTP)

AWS (AWS Logs,
FlowLogs, CloudTrail)

Beats/Logstash

JSON Path from HTTP
API

Plain/Raw Text (TCP,
UDP, AMQP, Kafka)





SYSLOG

Syslog RFC 5424:

```
$ 2003-10-11T22:14:15.003Z mymachine.example.com evntslog - ID47  
[exampleSDID@32473 iut="3" eventSource="Application"  
eventID="1011"] [examplePriority@32473 class="high"]
```

Syslog RFC 3164 (BSB)

```
$ Oct 22 10:52:12 scapegoat 1990 Oct 22 10:52:01 TZ-6  
scapegoat.dmz.example.org 10.1.2.3 sched[0]: That's All Folks!
```



DEMO SYSLOG





GELF(GRAYLOG EXTENDED LOG FORMAT)

- ✗ Resolve deficiências do syslog: Limitado à 1024 bytes.
- ✗ GELF é ótima opção para login de aplicação
- ✗ Facilidade de envio de *exceptions* para o Log
- ✗ Aceita compressão (GZIP)
- ✗ Evita carga de CPU
- ✗ Largura de rede



GELF (GRAYLOG EXTENDED LOG FORMAT)

```
{  
  "version": "1.1",  
  "host": "example.org",  
  "short_message": " DevOpsGo",  
  "full_message": "15° Devops GO: Graylog Trakif",  
  "timestamp": 1385053862.3072,  
  "level": 1,  
  "_user_id": 9001,  
  "_some_info": "foo",  
  "_some_env_var": "bar"  
}
```




GELF(GRAYLOG EXTENDED LOG FORMAT)

```
$ curl -XPOST http://graylog.example.org:12202/gelf -p0 -d  
'{"short_message":"Hello there", "host":"example.org",  
"facility":"test", "_foo":"bar"}'
```

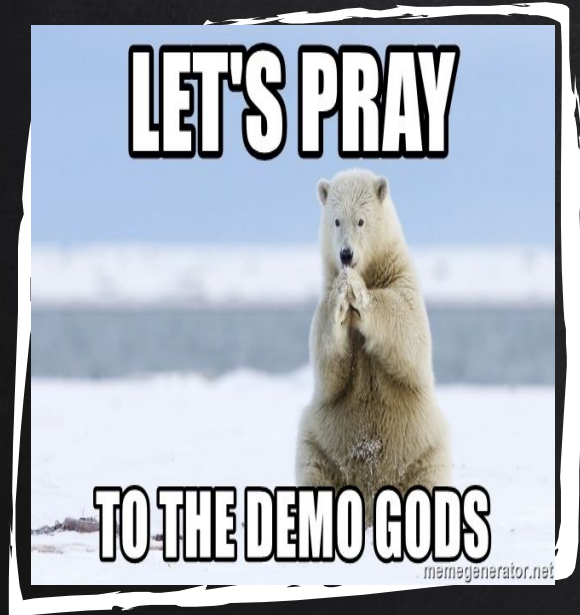



DEMO GELF



INPUTS

- ✗ Informa ao Graylog qual porta ficará em listen ou como recuperar as mensagens
- ✗ Coleta dados estruturados ou não-estruturados



DEMO INPUTS



STREAMS

Controlar o acesso à dados, análise, modificar e determinar mensagens arquivadas.

Router os dados e armazena em um índice

Router as mensagens em categorias real time

Streams

You can route incoming messages into streams by applying rules against them. Messages matching the rules of a stream are routed into it. A message can also be routed into multiple streams.

[Create Stream](#)

Read more about streams in the [documentation](#).

Filter streams

Filter

Reset

All messages

Index set *Default index set*

Default

Manage Rules

Manage Outputs

Manage Alerts

Pause Stream

More Actions ▾

Stream containing all messages

0 messages/second. The default stream contains all messages.

Stream-DevOps

Index set *Default index set*

Manage Rules

Manage Outputs

Manage Alerts

Pause Stream

More Actions ▾

StreamDevOps

0 messages/second. Must match all of the 1 configured stream rule. [Show stream rules](#)



DEMO STREAMS

DASHBOARD

- ✕ Widgets:
 - Search Result counts
 - Search Result histogram charts
 - Statistical value
- ✕ Field: counts, averages, total, trend indicators, charts, graphs, maps

Application overview

Overview of our most important application metrics

Drag widgets to any position you like in [unlock / edit mode](#).

[Update in background](#)[Fullscreen](#)[Unlock / Edit](#)

Total exceptions today

a few seconds ago

139,227



Failed DB queries last hour

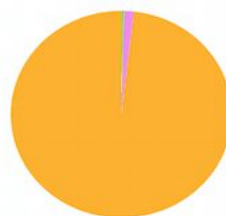
a few seconds ago

1,191



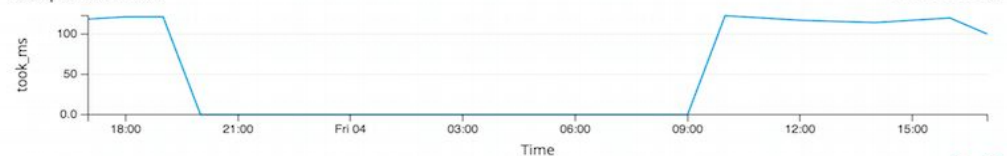
HTTP Response codes today

a few seconds ago



Value	%	Count
Top values		
200	98.19%	1,083
500	1.45%	16
504	0.36%	4

Response time



Total requests

a few seconds ago

975,829



User IDs

a few seconds ago

Value	%	Count
Top values		
6469981	56.03%	469,227
6476752	17.82%	149,242
9001	15.09%	126,421
74422	8.28%	69,328
54351	2.78%	23,298

Resources

a few seconds ago



Controllers

a few seconds ago

Value	%	Count
Top values		



DEMO DASHBOARD



RESUMO

Streams

São mecanismo de roteamento das mensagens;

Alerts

São baseados nas streams.
Você pode definir conditions e trigger alert

Dashboards

Dashboard permite criar visualizações pré definidas dos dados

Search

Graylog permite pesquisas personalizadas, com limitações de intervalo de tempo

Security

Permite você habilitar permissões de acessos com restrições.

Hundreds of Add-ons for Graylog.

How would you like to extend Graylog today?



Browse Add-ons by Type



Plugin




Content Pack



GELF Library



Other Solutions

 Search or jump to... / Pull requests Issues Marketplace Explore

bezarsnba / zabbix-graylog-monitoring

Press F11 to exit full screen

Unwatch 3 Unstar 8 Fork 1

Code Issues Pull requests Projects Wiki Insights Settings

No description, website, or topics provided.

Manage topics

15 commits 1 branch

Branch: master New pull request

- bezarsnba Fixed error SSL
- screenshot
- GrayLog-Nodes-1538687497927.json
- LICENSE
- README.md
- monitoring-graylog.py
- template_graylog-node.xml
- user_parameter_graylog.conf

README.md

GrayLog Node Mo

graylog Marketplace

Search Marketplace



Explore

Submit

Sign out

< Back to listing

Monitoring Graylog node using Zabbix

free!

Other Solutions

node graylog zabbix

bezarsnba

View on Github

0

☆

Published

03 Oct 07:07

Last Push

03 Oct 07:07

Readme from Github

GrayLog Node

Template created to monitor GrayLog

We added a feature of Zabbix called LLD (Low Level Discovery) in GrayLog, so that you do not have to

Monitoring Items:

Share

Zabbix templates, modules & more

Search...

Advanced Search

Applications

Anti-Virus

Backup

Bug and issue tracking

Cluster

Clustered File Systems

DNS

Firewall

HelpDesk System

High Availability (HA)

Java Application

Mail servers

Misc

Monitoring System

NTP

Others

Process Managers

Queue managers

Security

Skype

GrayLog Node Monitoring Using Zabbix

Template created to monitor GrayLog nodes through LLD (Low Level Discovery)

We added a feature of Zabbix called LLD (Low Level Discovery) in the model, this automation seeks to facilitate the discovery of the nodes in GrayLog, so that you do not have to register the nodes manually just set the time of the discovery rule.

Monitoring Items:

- GrayLog: Filter execution Time (Filtered, Incoming, Outgoing, Process)
- GrayLog: Internal Log Message (Error, Fatal, Trace, Warn)
- GrayLog: Journal (Journal Size)
- GrayLog: Node Memory(LLD)(Free Memory, Max Memory, Total Memory, Used Memory)
- GrayLog: Node Status (Lifecycle, Processing, Status)
- GrayLog: Services

Requirements

- Zabbix 3.4;
- Zabbix Agent install on Graylog;
- Python 3.4 or > Python3;
- Imports;
 - import requests;
 - import json;
 - import sys

1 vote Rating



THANKS!

Dúvidas?

@bezarsnba

bramos@onxsolutions.net

Linkedin

