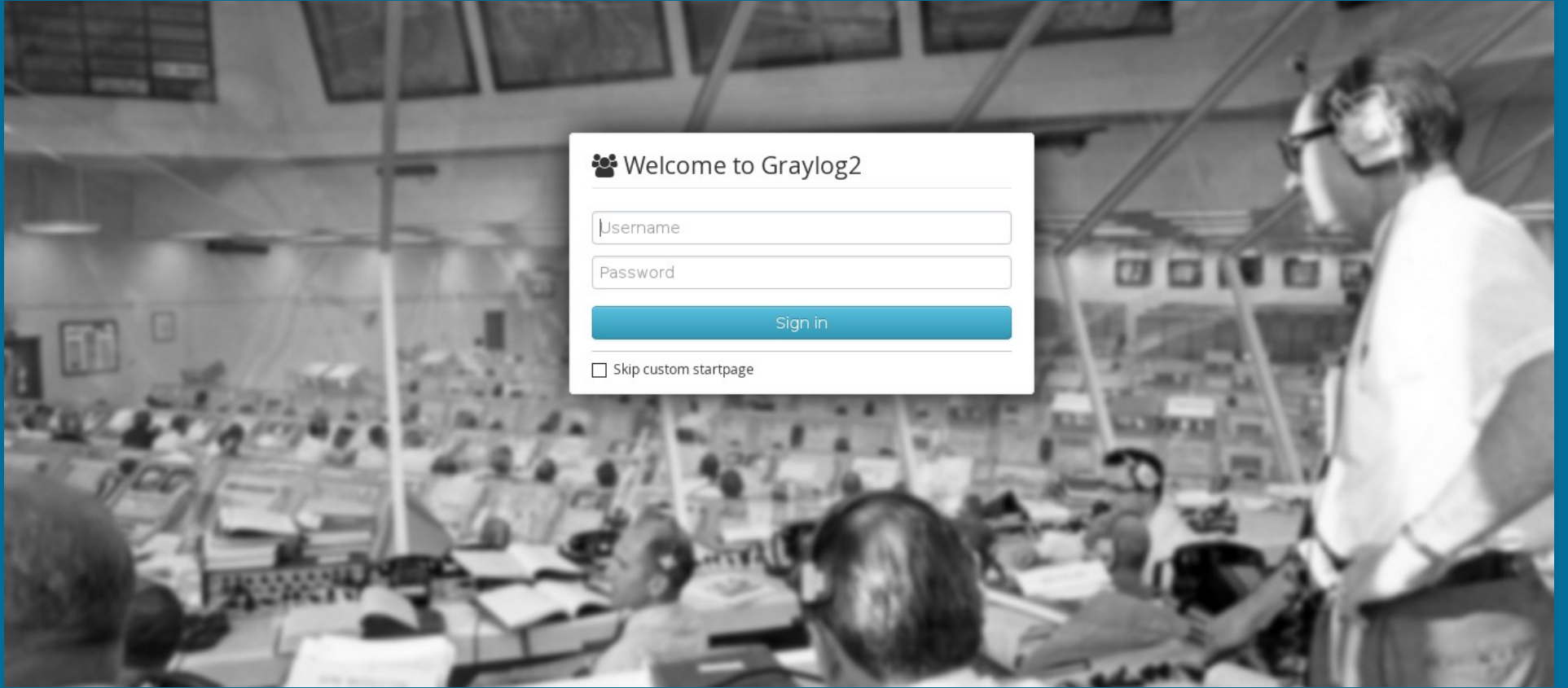


GRAYLOG2'DE EXTRACTOR İLE LOGLARIN AYRIŞTIRILMASI

Oğuzhan Coşkun | oguzhan.coskun@ozguryazilim.com.tr



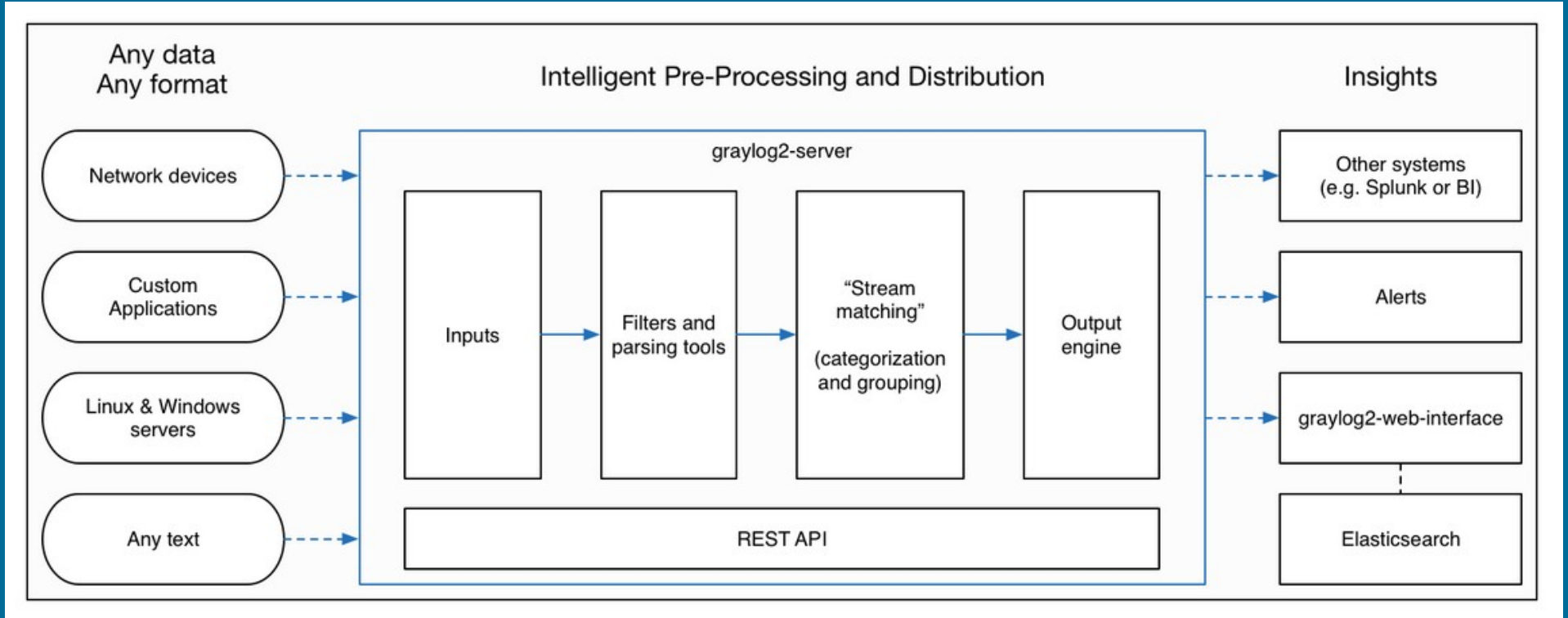


Kimdir, Nedir?

- Bir log analiz ve yönetim çözümüdür.
- 0.92.0 release sürümü 01-12-2014 tarihinde yayınlandı.
- GPL3 Lisanslı
- Gelen loglardan uyarılar üretip kullanıcılara bilgi verir.
- Farklı durumlara göre logların sınıflandırmasını yapabilir.



Nasıl Çalışır?



Extractors

- Nedir, Ne işe yarar?
 - Bir logun içerisinde size anlamlı gelen veriyi almak..

Warning: Invalid argument supplied for foreach() in /test.php on line 13



Extractors

- `Warning` // durum mesajı
- `test.php` // ilgili dizin-dosya
- `13` // ilgili satır



Extract Yöntemleri

- Substring
- Regular Expression
- Split & Index
- Copy Input



Regular Expression

```
^(((((((((\s? +)?\(((\s? +)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))\s? +)?|(\s? +)?([A-
Za-z0-9!#\!*\+V=?^`_{}~])+((((\s? +)?\
((\s? +)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s?
+)?\)))\s? +)?|(\s? +)?|((((\s? +)?\((\s?
+)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))
(\s? +)?|(\s? +)?"((\s? +)?(([\!#\-[ ]~])|(\[ [
-~]\s))))*(\s? +)?")?|((((\s? +)?\((\s?
+)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))
(\s? +)?|(\s? +)?<(((((\s? +)?\((\s? +)?
(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))\s?
+)?|(\s? +)?(([\A-Za-z0-9!#\!*\+V=?
^`_{}~])+\.( [\A-Za-z0-9!#\!*\+V=?^`_{}~])
+)*((((\s? +)?\((\s? +)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))\s? +)?|(\s? +)?|
((((\s? +)?\((\s? +)?(([\!-'\*-[\]-~]*)|(\[ [
-~]\s))))*(\s? +)?\)))\s? +)?|(\s? +)?"(\s?
+)?(([\!#\-[ ]~])|(\[ [
+)?\))) (...
```

[\\w\\-][\\w\\-\\.]+@[\\w\\-][\\w\\-\\.]+[a-zA-Z]{1,4}



Loglar Nereden Geliyor?

- Graylog2 logları nasıl ve nereden toplar?
 - Syslog, GELF, TCP, UDP,AMQP ile log alabilir.
- GELF?
 - Syslog gibi 1024 byte sınırı yok.
- Sistem Logları için Syslog, Uygulamalar için GELF



Audit Log

\$ModLoad imfile

\$InputFileName /var/log/audit/audit.log

\$InputFileTag Auditd

\$InputFileStateFile /var/spool/rsyslog

\$InputFileFacility local4

\$InputRunFileMonitor

local4.* @127.0.0.1:15514



Audit Extractor (JSON)

```
{
  "extractors": [
    {
      "condition_type": "none",
      "condition_value": "",
      "converters": [],
      "cursor_strategy": "copy",
      "extractor_config": {
        "regex_value": "\\w+\\s+useradd.*name=(\\w+)"
      },
      "extractor_type": "regex",
      "order": 0,
      "source_field": "message",
      "target_field": "Useradd",
      "title": "Useradd Name"
    }
  ],
  "version": "0.91.3"
}
```



Extractors (WUI)

The screenshot shows the Graylog2 web interface for configuring a new extractor. The browser address bar shows the URL: `https://graylog2.example.org/system/inputs/3c1749a2-b7ae-4e23-b761-f0b666e50e36/52f007d2e4b0fa0558898b9b/extractors/new?extractor_type...`. The page title is "New extractor for input Syslog". The type is "Regular expression" and the field is "message". A sample log message is shown: `mgmt-mongo sshd[16144]: Invalid user oracle from 183.100.212.37`. The regular expression is `]: Invalid user (.*?)s/w`. The "Always try to extract" option is selected. The field name is `ssh_invalid_username`. The "Copy" option is selected for "Do you want to copy or cut from source?". The extractor title is `sshd invalid username`. The converter is set to "Numeric".

System / Nodes / 3c1749a2 / Input: Syslog / Extractors

New extractor for input Syslog

Type: Regular expression, Field: message

```
mgmt-mongo sshd[16144]: Invalid user oracle from 183.100.212.37
```

Regular expression:

 [Try!](#)

The regular expression used for extraction. First matcher group is used.

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.

Store as field:

Choose a field name. The extracted value will be stored in it. Call it `http_response_code` for example if you are extracting a HTTP response code.

Copy Cut

Do you want to copy or cut from source?

Extractor title:

A descriptive name of this extractor.

Add converter:

 [Add](#)

SYSTEM

- Overview
- Nodes
- Inputs
- Indices
- Logging
- Users

Extractors (WUI)

The screenshot shows the Graylog2 search results page. The search query is 'heroku'. The interface includes a search bar, a histogram showing the distribution of results over time, and a table of search results. The histogram shows a peak in activity around 14:00. The table lists search results with columns for Timestamp, Source, Message, http_status, and request_id.

Search results
Found 80,146 messages.

Total result histogram

Resolution: Year, Quarter, Month, Week, Day, Hour, Minute

Timestamp	Source	Message	http_status	request_id
2014-05-20 03:39:57.284	www.graylog2.org	at=info method=GET path=/ host=www.graylog2.org request_id=f3ffb87e-b9f8-4b74-ac41-b762f1564f88 8 fwd="164.177.1.1" dyno=web.1 connect=0ms service=4ms status=200 bytes=31094	200	f3ffb87e-b9f8-4b74-ac41-b762f1564f88
2014-05-20 03:39:56.752	www.graylog2.org	at=info method=GET path=/ host=www.graylog2.org request_id=a8dedfc9-0e9d-49f4-b7ef-7b2167249e30 fwd="54.253.1.1" dyno=web.1 connect=0ms service=8ms status=200 bytes=31094	200	a8dedfc9-0e9d-49f4-b7ef-7b2167249e30

Message details:
Received by Heroku test 2 on P3c1749a2 / 54.247.1.1
Timestamp: 2014-05-20 03:39:57.284
Index: graylog2_1

Actions

bytes
31094

client_ip
164.177.1.1

connect_time_ms
0

drain_id
d.158ca493-4116-451a-9e6e-8158d609eb53

dyno
web.1

facility
local3

heroku_component
router

heroku_source_type
heroku

http_method
get

http_status
200

level
Info [6]

message
at=info method=GET path=/ host=www.graylog2.org request_id=f3ffb87e-

Katkıda Bulunmak

Data Source Library

This should not be regarded as a complete list. For example, the specific firewall you use is not listed below because it uses RFC compatible syslog that is supported by the standard Graylog2 syslog input.

Show: 15 ▾

Search:

Title	Type	Author
.NET/log4net (gelf4net) 	GELF library	jjchiw
.NET/NLog (Gelf4NLog) 	GELF library	Ozan Seymen
.NET/NLog (NLog.GelfLayout) 	GELF library	Farzad Panahi
Apache AccessLog	Extractor	Oguzhan Coskun (Özgür Yazılım A.Ş.)
Audit Daemon	Extractor	Oguzhan Coskun (Özgür Yazılım A.Ş.)
AWS CloudTrail beta	Input plugin	Lennart Koopmann (TORCH GmbH)
Bind9 Query Log	Extractor	Richard Hope
C++ (gelf4cplus) 	GELF library	Steven Bidny



ÖRNEK



Özgür Yazılım A.Ş.
www.ozguryazilim.com.tr

Teşekkürler

Soru ve önerileriniz için;

<http://seminer.linux.org.tr/iletisim/>

oguzhancoskun.org | [@oguzhancoo](https://twitter.com/oguzhancoo)