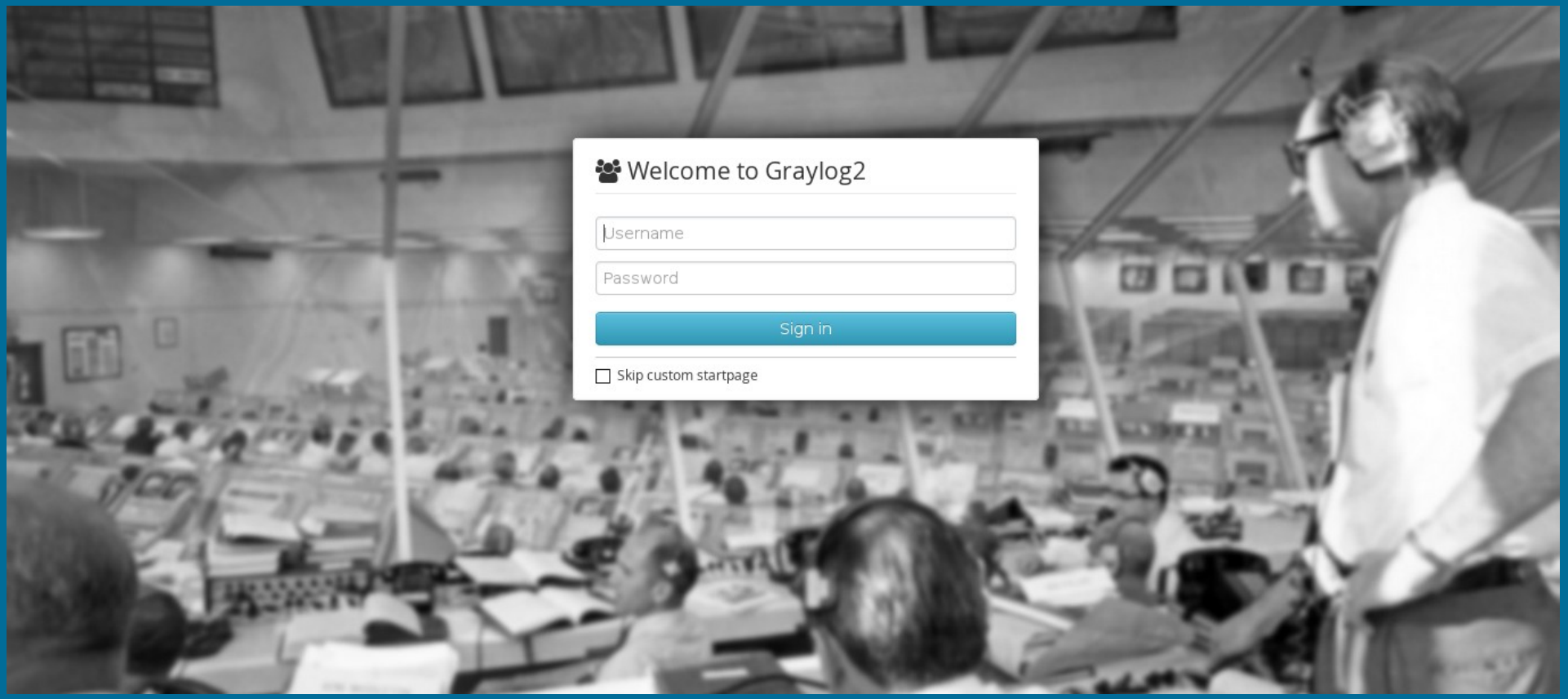
GRAYLOG2'DE EXTRACTOR İLE LOGLARIN AYRIŞTIRILMASI

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

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

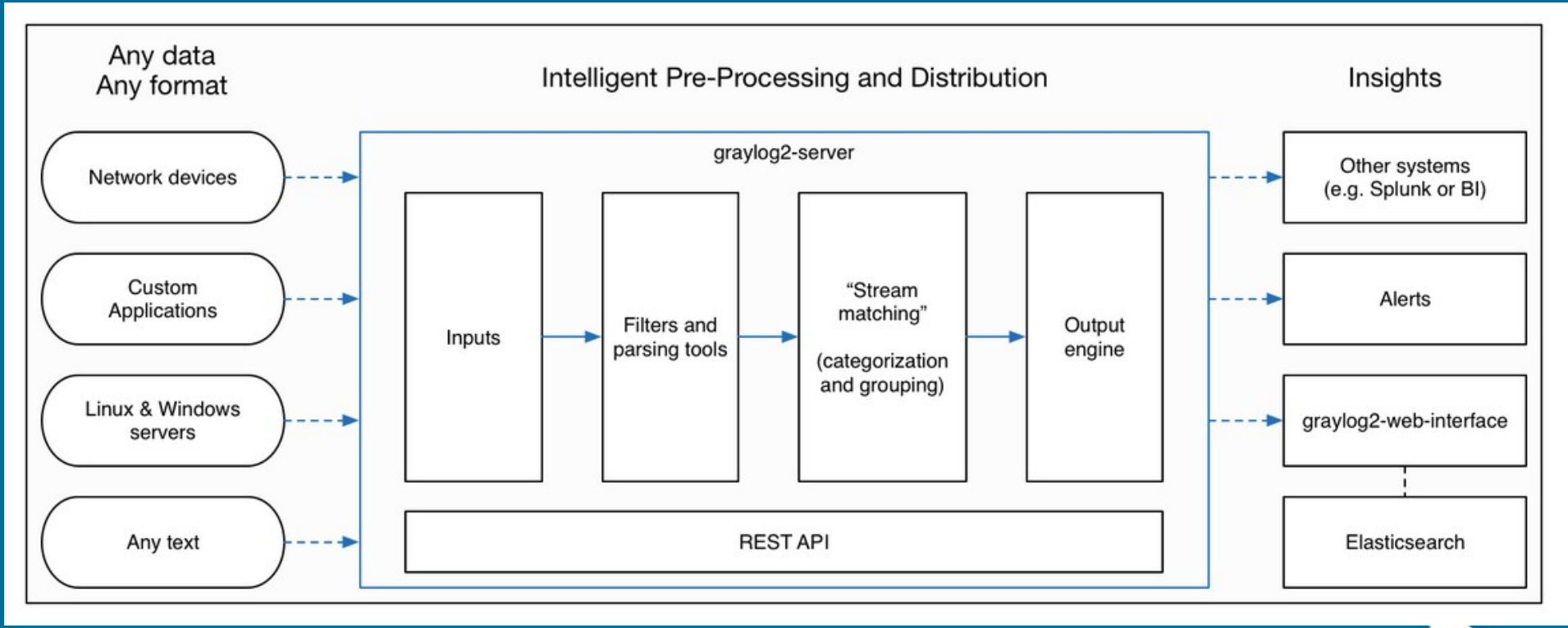


Özgür Yazılım A.Ş.
www.ozguryazilim.com.tr

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

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

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

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

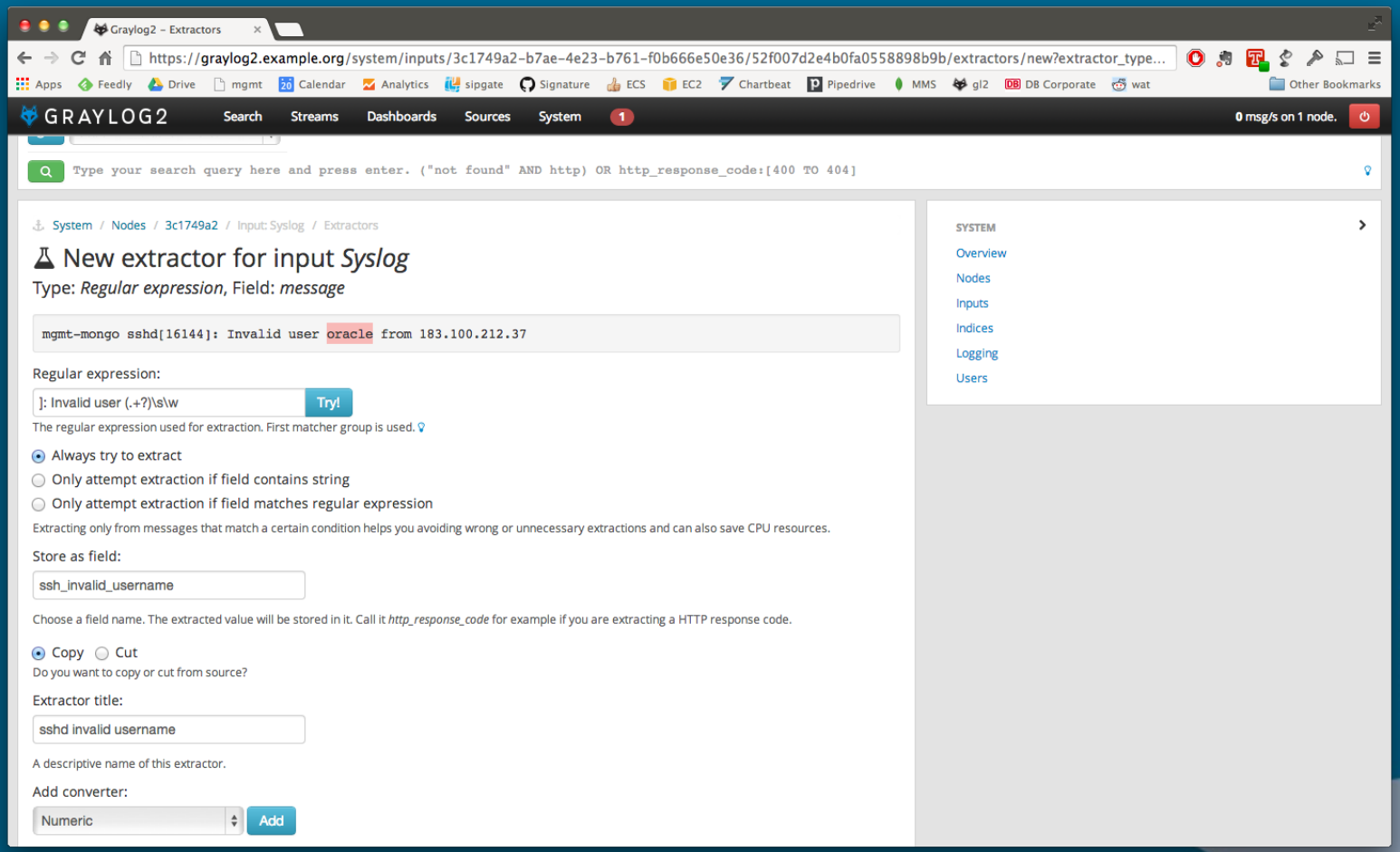
```
$ModLoad imfile
$InputFileName /var/log/audit/audit.log
$InputFileTag Auditd
$InputFileStateFile /var/spool/rsyslog
$InputFileFacility local4
$InputRunFileMonitor

local4.* @127.0.0.1:15514
```

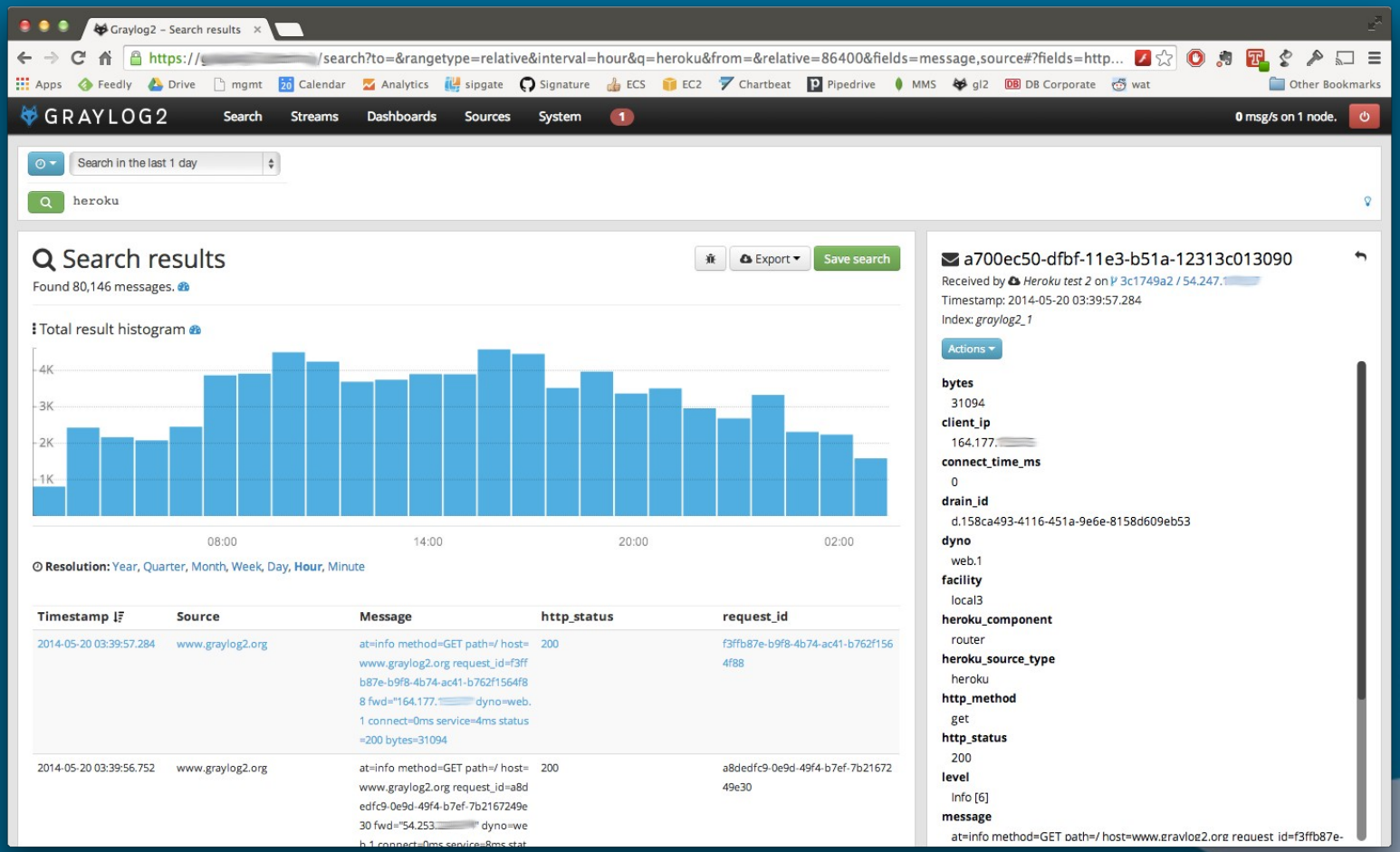
Audit Extractor (JSON)


```
{
  "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)



Extractors (WUI)



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