# Online Grok Pattern Generator / Debugger Tool



Grok is a term coined by American writer Robert A. Heinlein for his 1961 science fiction novel Stranger in a Strange Land.
When using the ELK stack we are ingesting the data to elasticsearch, the data is initially unstructured. We first need to break the data into structured format and then ingest it to elasticsearch. Such data can then be later used for analysis. This data manipualation of unstructured data to structured is done by Logstash. Logstash itself makes use of grok filter to achieve this.
While the Oxford English Dictionary summarizes the meaning of grok as "to understand intuitively". Grok works by combining text patterns into something that matches your logs. This tool is perfect for syslog logs, apache and other webserver logs, mysql logs, and in general, any log format that is generally written for humans and not computer consumption. Logstash ships with about 120 patterns by default.

GROK

**Enter the log -**

```
17-07-2022 12:46:56.636 [http-nio-8085-exec-1] INFO
c.demo.ELK.controller.ELKController.helloWorld - Response => Hello World! Sun Jul
17 12:46:56 GMT 2022
```

Log data which is to be structured using grok pattern. Example - **2016-07-11T23:56:42.000+00:00 INFO [com.javainuse]:Transaction with transactionid-10 took 10 ms**

**Enter the grok pattern -**

```
grok { match => { "message" => "%{TIMESTAMP_ISO8601:timestamp} %
{LOGLEVEL:log-level} \[%{DATA:issuer}\]:%{GREEDYDATA:message}" }
 }
```

The syntax for a grok pattern is %{SYNTAX:SEMANTIC} The SYNTAX is the name of the pattern that will match your text. The SEMANTIC is the identifier given to a matched text. Example - **%{TIMESTAMP_ISO8601:timestamp}**

Test Grok

```
(?<name12>.*)" }
 }
    ^
```

# Commonly used Logstash Grok Pattern Examples

- Example 1

  Use of grok sematic - NUMBER and IP

  **Application Log -**

  ```
  64.3.89.2 took 300 ms
  ```

Close X

```
filter {
 grok { match => { "message" => "%{IP:client} took %{NUMBER:duration}" }
 }
}
```

**Output -**

```
{
  "duration": "300",
  "client": "64.3.89.2"
}
```

- Example 2

Use of grok sematic - TIMESTAMP,LOGLEVEL,DATA and GREEDYDATA

**Application Log -**

```
2020-03-11T17:23:34.000+00:00 WARNING [App.DataService]:Transaction failed for transa
```

**Grok Pattern -**

```
filter {
 grok { match => { "message" => "%{TIMESTAMP_ISO8601:timestamp} %{LOGLEVEL:log-level}
 }
}
```

**Output -**

```
{
  "YEAR": "2020",
  "MONTHNUM": "03",
  "HOUR": [
    "17",
    "00"
  ],
  "log-level": "WARNING",
  "MINUTE": [
    "23",
    "00"
  ],
  "SECOND": "34.000",
  "message": "Transaction failed for transaction id -4jsdf94jsdf29msdf92",
  "ISO8601_TIMEZONE": "+00:00",
  "MONTHDAY": "11",
```

Close X

- Example 3

Grok fields are strings by default. Numeric fields (int and float) can be declared in the pattern

**Application Log -**

```
Transaction id 567
```

**Grok Pattern -**

```
filter {
 grok { match => { "message" => "%{TIMESTAMP_ISO8601:timestamp} Transaction id %{USER
 }
}
```

**Output -**

```
{"transactionid": 567}
```

## Related Posts

- Spring Boot Microservices + ELK Stack Hello World Example (/spring/springboot-microservice-elk)
- File Beat + ELK(Elastic, Logstash and Kibana) Stack to index logs to Elasticsearch - Hello World Example (/elasticsearch/filebeat-elk)

Search Tutorials

## Other Online tools

- Online JWT Generator (/jwtgenerator)
- Online JWT Decoder (/decodeJWT)
- Online Bcrypt Generator and Validator (/onlineBcrypt)
- Online tool to generate and check MD5 hashed passwords (/onlinemd5)
- Online Hex Encoder and Decoder Tool (/onlinehex)
- Online HTML Encoder Tool (/onlinehtmlencode)
- Online HTML Decoder Tool (/onlinehtmldecode)

- Online PGP Encryption, Decryption And Key Generator Tool (/pgpgenerator)
- Online Triple DES Encryption and Decryption Tool (/desgenerator)
- Online HMAC Generator Tool (/hmac)
- Online tool to generate and decrypt/check Jasypt encrypted passwords (/jasypt)
- Online Grok Pattern Generator Tool (/grok)
- Online JSONPath Evaluator Tool (/jsonpath)
- Online Tool To Convert XML To JSON And JSON To XML (/xmljson)
- Java Decompiler Online (/decomp)
- Online JSON to Java POJO Class Converter (/pojo)
- Online Text(String) Size Calculator Tool (In Bytes) (/bytesize)
- JSON to NDJSON Online Converter Tool (/ndjson)
- Cron Expression Generator Tool (/cron)
- JSON to YAML Converter Tool (/jsontoyaml)
- YAML to JSON Converter Tool (/yamltojson)
- YAML to POJO Converter Tool (/yamltopojo)
- XML to POJO Converter Tool (/xmltopojo)
- Online Regex Generator Tool (/rexgenerator)
- Online Regex Tester and Debugger Tool (/regtester)
- Online Bash Shell Scripts to Windows Batch Files Converter Tool (/createbash)