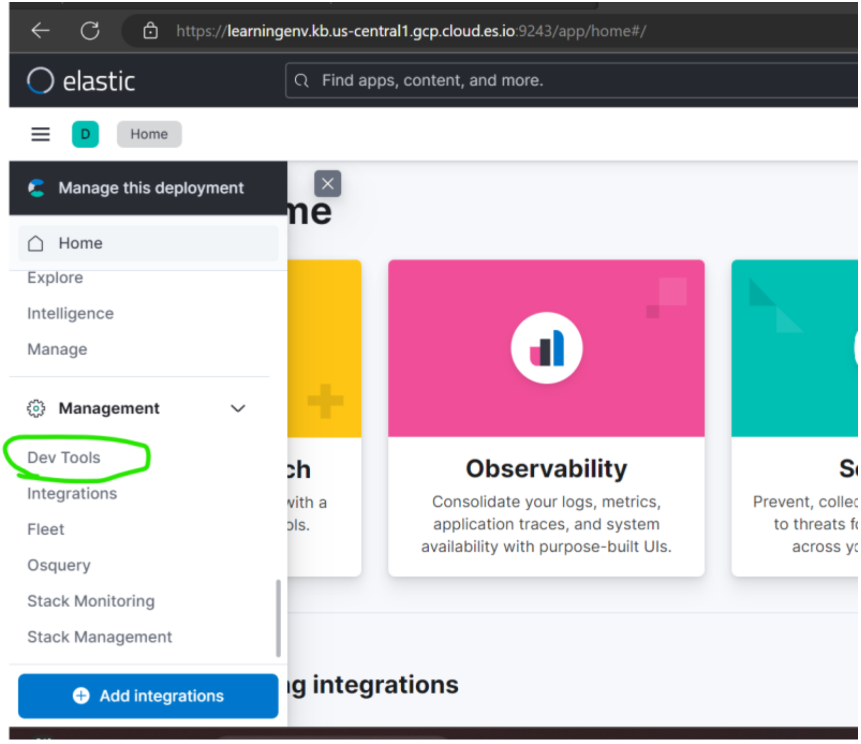
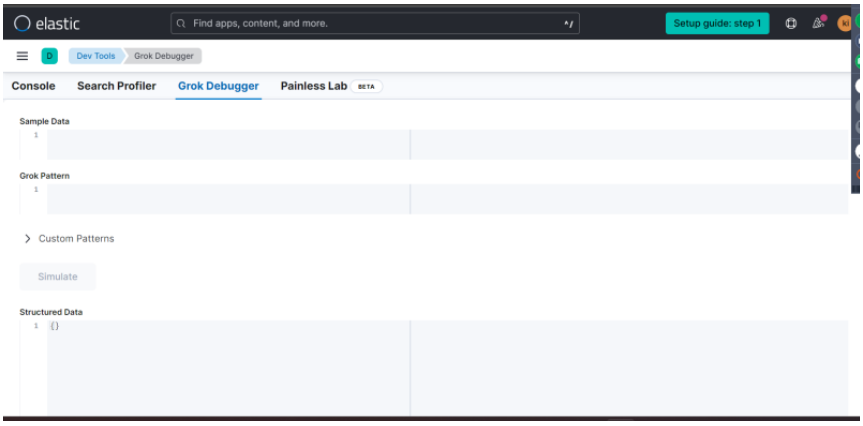
MAY 18, 2023

DevOps Classroomnotes 18/May/2023

Grok Patterns

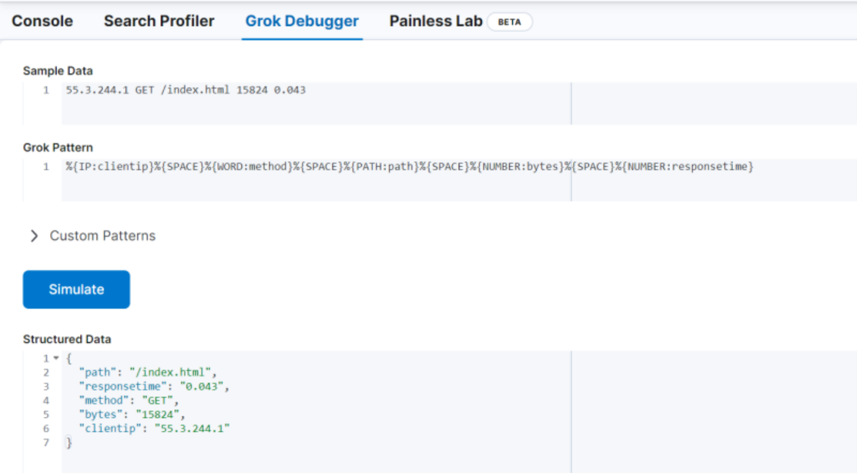
- Open the DevTools in Kibana and then Grok Debugger





- Refer Here for the grok filter in logstash
- For writing your own patterns use regex Refer Here

- Lets try to build a simple pattern as shown below



Sample Data

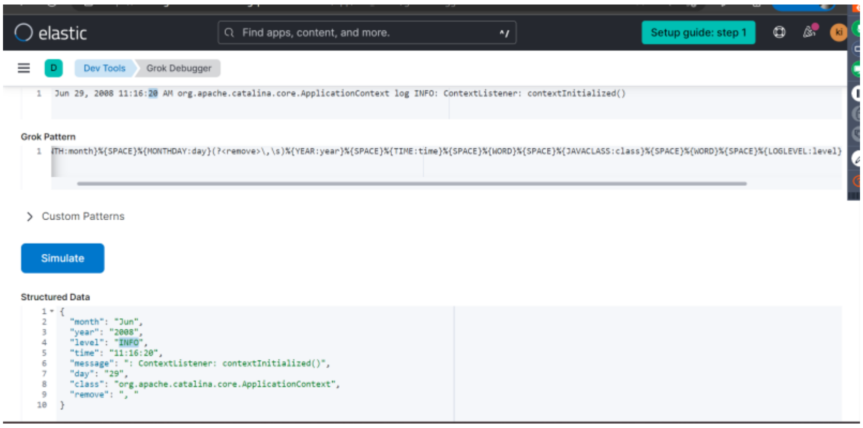
```
55.3.244.1 GET /index.html 15824 0.043
```

Grok Pattern

```
%{IP:clientip}%{SPACE}%{WORD:method}%{SPACE}%{PATH:path}%{SPACE}%{NUMBER:bytes}%{SPACE}%{NUMBER:responsetime}
```

Structured Data

```
{
  "path": "/index.html",
  "responsetime": "0.043",
  "method": "GET",
  "bytes": "15824",
  "clientip": "55.3.244.1"
}
```



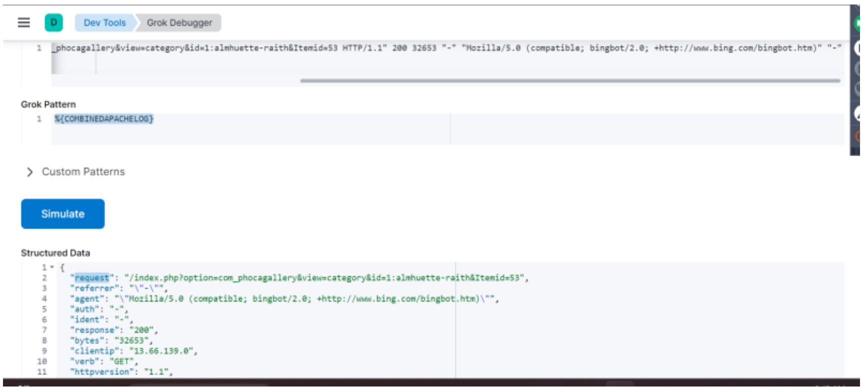
```
Jun 29, 2008 11:16:20 AM org.apache.catalina.core.ApplicationContext log INFO: ContextListener: contextInitialized()
```

Grok Pattern

```
TH:month}%{SPACE}%{MONTHDAY:day}(?<remove>\,\s)%{YEAR:year}%{SPACE}%{TIME:time}%{SPACE}%{WORD}%{SPACE}%{JAVACLASS:class}%{SPACE}%{WORD}%{SPACE}%{LOGLEVEL:level}
```

Structured Data

```
{
  "month": "Jun",
  "year": "2008",
  "level": "INFO",
  "time": "11:16:20",
  "message": ": ContextListener: contextInitialized()",
  "day": "29",
  "class": "org.apache.catalina.core.ApplicationContext",
  "remove": ", "
}
```



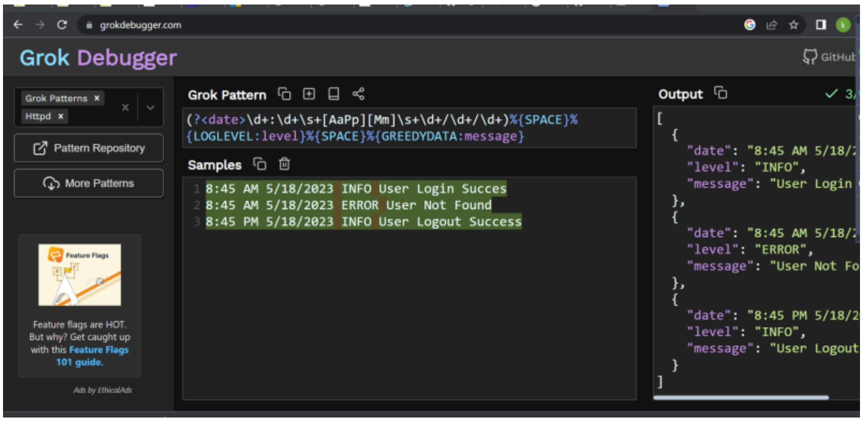
```
_phocagallery&view=category&id=1:almhuette-raith&Itemid=53 HTTP/1.1" 200 32653 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)" "-"
```

Grok Pattern

```
%{COMBINEDAPACHELOG}
```

Structured Data

```
{
  "request": "/index.php?option=com_phocagallery&view=category&id=1:almhuette-raith&Itemid=53",
  "referrer": "\"-\"",
  "agent": "\"Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)\"",
  "auth": "-",
  "ident": "-",
  "response": "200",
  "bytes": "32653",
  "clientip": "13.66.139.0",
  "verb": "GET",
  "httpversion": "1.1",
```



Grok Pattern

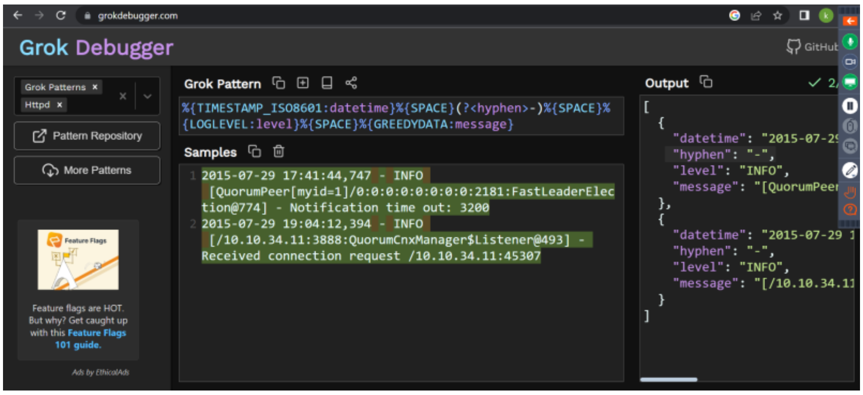
```
(?<date>\d+:\d+\s+[AaPp][Mm]\s+\d+/\d+/\d+)%{SPACE}%
{LOGLEVEL:level}%{SPACE}%{GREEDYDATA:message}
```

Samples

```
8:45 AM 5/18/2023 INFO User Login Succes
8:45 AM 5/18/2023 ERROR User Not Found
8:45 PM 5/18/2023 INFO User Logout Success
```

Output

```
[
  {
    "date": "8:45 AM 5/18/2
    "level": "INFO",
    "message": "User Login
  },
  {
    "date": "8:45 AM 5/18/2
    "level": "ERROR",
    "message": "User Not Fo
  },
  {
    "date": "8:45 PM 5/18/2
    "level": "INFO",
    "message": "User Logout
  }
]
```



Grok Pattern

```
%{TIMESTAMP_ISO8601:datetime}%{SPACE}(?<hyphen>-)%{SPACE}%
{LOGLEVEL:level}%{SPACE}%{GREEDYDATA:message}
```

Samples

```
2015-07-29 17:41:44,747 - INFO
 [QuorumPeer[myid=1]/0:0:0:0:0:0:0:0:2181:FastLeaderElec
tion@774] - Notification time out: 3200
2015-07-29 19:04:12,394 - INFO
 [/10.10.34.11:3888:QuorumCnxManager$Listener@493] -
Received connection request /10.10.34.11:45307
```

Output

```
[
  {
    "datetime": "2015-07-2
    "hyphen": "-",
    "level": "INFO",
    "message": "[QuorumPeer
  },
  {
    "datetime": "2015-07-29 1
    "hyphen": "-",
    "level": "INFO",
    "message": "[/10.10.34.11
  }
]
```

- Refer Here for grok debugger

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.

About continuous learner

devops & cloud enthusiastic learner

VIEW ALL POSTS

PREVIOUS POST

Azure Classroomnotes 18/May/2023

NEXT POST

AWS Classroomnotes 18/May/2023

POWERED BY WORDPRESS.COM.