



MAY 17, 2023

DevOps Classroomnotes 17/May/2023

Logstash

- Lets create a linux vm and explore logstash

Logstash pipeline:

- Logstash pipeline syntax

```
input {}
filter {}
output {}
```

- In input section we can define the datasources from where we process inputs Extract
- In Filter section we define the transformations Transform
- In output section we define the destination Load
- The list of inputs is all the installed logstash input plugins and same with other sections

Lets create a very basic pipeline which reads input from stdin and displays out to stdout

- Stdin input plugin [Refer Here](#)
- Stdout output plugin [Refer Here](#)
- Pipeline

```
input {
  stdin {
  }
}
output {
  stdout {
  }
}
```

- Create a file with above content in /tmp/first.conf
- cd in /usr/share/logstash and execute the following command `sudo ./bin/logstash -f /tmp/first.conf`

```
pipelines_running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}

this is my first input
{
  "host" => {
    "hostname" => "ip-172-31-8-162"
  },
  "@version" => "1",
  "message" => "this is my first input",
  "@timestamp" => 2023-05-17T03:01:51.185072690Z,
  "event" => {
    "original" => "this is my first input"
  }
}
```

- Now lets the codec from rubydebug to json
- Edit first.conf with following content and start logstash `sudo ./bin/logstash -f /tmp/first.conf`

```
input {
  stdin {
  }
}
output {
  stdout {
    codec => json
  }
}
```

```
[INFO ] 2023-05-17 03:12:47.741 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[:main], :non_running_pipelines=>[:]}
this is my first message
{"event":{"original":"this is my first message"},"host":{"hostname":"ip-172-31-8-162"},"@version":
"1","message":"this is my first message","@timestamp":"2023-05-17T03:06:03.596463408Z"}
```

* Lets add one more output to some file `stdout => codec => rubydebug

* [Refer Here](#) for file output plugin

```
input {
  stdin {
  }
}
output {
  stdout {
  }
  file {
    path => "/tmp/output%{+YYYY-MM-dd}.txt"
  }
}
```

```
The stdin plugin is now waiting for input:
[INFO ] 2023-05-17 03:12:47.741 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[:]}
this is my first message
{
  "host" => {
    "hostname" => "ip-172-31-8-162"
  },
  "message" => "this is my first message",
  "@version" => "1",
  "event" => {
    "original" => "this is my first message"
  },
  "@timestamp" => 2023-05-17T03:13:00.022994124Z
}
[INFO ] 2023-05-17 03:13:00.173 [[main]worker1] file - Opening file {:path=>"/tmp/output2023-05-17.txt"}
hello, how are you?
{
  "host" => {
    "hostname" => "ip-172-31-8-162"
  },
  "message" => "hello, how are you?",
  "@version" => "1",
  "event" => {
    "original" => "hello, how are you?"
  },
  "@timestamp" => 2023-05-17T03:13:12.546796332Z
}
```

* Open the file for contents

```
ubuntu@ip-172-31-8-162:/usr/share/logstash$ cat /tmp/output2023-05-17.txt
{"host":{"hostname":"ip-172-31-8-162"},"message":"this is my first message","@version":"1",
,"event":{"original":"this is my first message"},"@timestamp":"2023-05-17T03:13:00.022994124Z"}
{"host":{"hostname":"ip-172-31-8-162"},"message":"hello, how are you?","@version":"1","event":{"original":"hello, how are you?"},"@timestamp":"2023-05-17T03:13:12.546796332Z"}
ubuntu@ip-172-31-8-162:/usr/share/logstash$
```

Activity 2: Lets create a pipeline to read the file /tmp/test and display the contents in stdout

- input = file
- output = stdout

```
input {
  file {
    path => ["/tmp/test"]
  }
}
output {
  stdout {
  }
}
```

- install apache and redirect /var/log/apache2/access.log to stdout

```
input {
  file {
    path => ["/var/log/apache2/access.log"]
  }
}
output {
  stdout {
  }
}
```

- Lets try to understand filters.
- Grok filter can parse unstructured data into fields [Refer Here](#)

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 17/May/2023](#)

[NEXT POST](#)

[AWS Classroomnotes 17/May/2023](#)

POWERED BY [WORDPRESS.COM](#).