【logstash】常用語法

基本架構

```
input {
   #輸入插件
}
filter {
   #□□匹配插件
}
output {
   #輸出插件
}
```

---

filter

超過長度截斷訊息

```
if [message] {
      if [message] =~ /.{4000,}/ {
      ## 刪除
      # drop {}
      # 超出長度截斷
       ruby {
          code => "event.set('message', event.get('message')[0..4000])"
       }
       # 新增truncated欄位，標記是否有截斷
        mutate {
          add_field => { "truncated" => "true" }
        }
      } else {
        mutate {
          add_field => { "truncated" => "false" }
        }
      }
  }
```

⏲修訂版本 #2
★由 treeman 建立於 9 ◆Q◆◆ 2024 10:57:33
✎由 treeman 更新於 9 ◆Q◆◆ 2024 11:08:37