

【Treeman】ELK相關

- [Logstash](#)
 - [【logstash】常用語法](#)
 - [【Logstash】相關資源](#)

Logstash

【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" }  
    }  
  }  
}
```

【Logstash】相關資源

- grok pattern 測試頁面
<http://grokconstructor.appspot.com/do/match>
- logstash基礎學習
<https://www.cnblogs.com/xiaoyh/p/16270512.html>
<https://www.cnblogs.com/xiaoyh/p/16270516.html>
<https://www.cnblogs.com/xiaoyh/p/16271608.html>
- **Logstash Pattern 簡單教學**
https://mmx362003.gitbooks.io/elk-stack-guide/content/config_of_logstash.html