



我會告訴你 Logstash 的流程，請依據以下條件幫我產生對應的 pipeline.conf

- Logstash 須從 Azure EventHub 讀取 JSON 格式的 log 資料
- 將 log 資料的屬性 "created" 轉成 "timestamp"
- 過濾掉 log 資料的屬性 "response.headers" 以及 "response.body"
- 根據屬性 "service\_name" 設定寫入 Elasticsearch 的 index，須加上寫入時的西元年跟週數，範例格式如 "myservice-2023.09"
- 處理完的資料送到 Elasticsearch



根據您提供的需求，以下是一個可能的 pipeline.conf 檔案：

javascriptCopy code

```
input {
  eventhub {
    connectionString => "Endpoint=sb://[your_eventhub_namespace].servicebus.windows.net/[your_eventhub_name];EntityName=[your_eventhub_name];"
    consumerGroup => "$Default"
    codec => json
  }
}

filter {
  mutate {
    rename => { "created" => "timestamp" }
  }
  prune {
    blacklist_names => ["response.headers", "response.body"]
  }
  if [service_name] {
    mutate {
      add_field => { "index" => "%{service_name}-%{+Y}.$week_of_year" }
    }
  }
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "%{index}"
  }
}
```

上述設定中的 `input` 區塊會從 Azure EventHub 讀取 JSON 格式的 log 資料，並使用 `codec => json` 指定資料編碼方式。 `filter` 區塊中的 `mutate` 則會將 "created" 屬性更名為 "timestamp"，而 `prune` 則會過濾掉 "response.headers" 和 "response.body" 屬性。接下來的 `if` 條件則會根據 "service\_name" 屬性的值加上特定的 index 名稱，透過 Elasticsearch 的格式來紀錄資料。最後， `output` 區塊會將處理過的資料送到 Elasticsearch 中。