

 免費電子書

學習

logstash

Free unaffiliated eBook created from
Stack Overflow contributors.

#logstash

.....	1
1: logstash	2
.....	2
Examples.....	2
.....	2
Syslog.....	2
ElasticSearch.....	2
.....	4

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: [logstash](#)

It is an unofficial and free logstash ebook created for educational purposes. All the content is extracted from [Stack Overflow Documentation](#), which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official logstash.

The content is released under Creative Commons BY-SA, and the list of contributors to each chapter are provided in the credits section at the end of this book. Images may be copyright of their respective owners unless otherwise specified. All trademarks and registered trademarks are the property of their respective company owners.

Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

1: logstash

logstash。

logstash。 logstash。

Examples

logstash。

Syslog

Logstash。 ◦

```
input {
  file {
    path => [
      "/var/log/syslog",
      "/var/log/auth.log"
    ]
    type => "syslog"
  }
}

filter {
  if [type] == "syslog" {
    # Uses built-in Grok patterns to parse this standard format
    grok {
      match => {
        "message" => "%{SYSLOGBASE}%{SPACE}%{GREEDYDATA:SYSLOGMESSAGE}"
      }
    }
    # Sets the timestamp of the event to the timestamp of recorded in the log-data
    # By default, logstash sets the timestamp to the time it was ingested.
    date {
      match => [ "timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}

output {
  # Outputs processed events to an elasticsearch instance local to the box.
  elasticsearch {
    hosts => [
      "localhost"
    ]
  }
}
```

ElasticSearch

ElasticSearch。

◦ ElasticSearch◦ ElasticSearch◦ elasticsearch {}◦ ◦

```
output {
  if [type] == 'metrics' {
    # The 'metrics' index rotates weekly.
    # The 'metrics-mapping.json' file defines the custom mappings.
    elasticsearch {
      hosts          => [ 'localhost' ]
      index          => "metrics-%{xxxx.wd}"
      manage_template => true
      template       => "/etc/logstash/metrics-mapping.json"
      template_overwrite => true
    }
  }
}
```

metricsmetrics-metricsISO◦ ◦ ◦ ◦

QAElasticSearchLogStashElasticSearch◦

logstash <https://riptutorial.com/zh-TW/logstash/topic/6903/logstash>

S. No		Contributors
1	logstash	Community , sysadmin1138