無料電子ブック

学習

logstash

Free unaffiliated eBook created from
Stack Overflow contributors.

#logstash

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.

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をいめる

このセクションでは、logstashのと、がそれをいたいについてします。

また、logstashのきなテーマについてもし、するトピックにリンクしてください。 logstashのドキュメンテーションはしいので、これらのトピックのバージョンをするがあります。

Examples

インストールまたはセットアップ

ログ･スタッシュをセットアップまたはインストールするためのしい。

なSyslogの

Logstashには、そのにち、syslogデータをしてするがあります。このは、なをしています。

```
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へののインデックスとマッピング

によっては、ElasticSearchののインデックスにするがあるか、またはしいインデックスがロールインするときにするカスタムマッピングをとすることがあります。

カスタムマッピングをするは2つあります。 1つのは、ElasticSearchテンプレートをアップロードすることです。それについては、ElasticSearchのドキュメントをしてください。もう1つのは、`elasticsearch {}`にマッピングをすることです。それがここにされているものです。

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

これにより、 `metrics-` `metrics`インデックスに`metrics`イベントがされ`metrics`このインデックスは、ISOをしてします。しいにされるテンプレートは、こののとしてされています。テンプレートをすることは、フィールドのタイプをタイプにするがあります。これは、のタイプがフィールドをわずかになるデータタイプとしてしようとするよりきいでにちます。

ElasticSearchテンプレートはLogStashコードでされており、ElasticSearchクラスタのとしてするがないため、このはステージングおよびQAでちます。

オンラインでlogstashをいめるをむ https://riptutorial.com/ja/logstash/topic/6903/logstashをいめる

クレジット

S. No		Contributors
1	logstashをいめる	Community, sysadmin1138