EBook Gratis

APRENDIZAJE logstash

Free unaffiliated eBook created from
Stack Overflow contributors.

#logstash

Tabla de contenido

Acerca de

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

Capítulo 1: Empezando con logstash

Observaciones

Esta sección proporciona una descripción general de qué es logstash, y por qué un desarrollador puede querer usarlo.

También debe mencionar cualquier tema grande dentro de logstash, y vincular a los temas relacionados. Dado que la Documentación para logstash es nueva, es posible que deba crear versiones iniciales de esos temas relacionados.

Examples

Instalación o configuración

Instrucciones detalladas sobre cómo configurar o instalar logstash.

Un ejemplo básico, completo de Syslog

A sus raíces, Logstash tiene la capacidad de analizar y almacenar datos de syslog. Este ejemplo muestra una configuración básica que te lleva a eso.

```
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"
    ]
  }
}
```

Salida a ElasticSearch: múltiples índices y mapeos

A veces, es necesario enviar a más de un índice en ElasticSearch o tener un mapeo personalizado que desee aplicar a los nuevos índices a medida que avanzan.

Hay dos formas de aplicar un mapeo personalizado. Una forma, es subir una plantilla de ElasticSearch. Vea la documentación de ElasticSearch para eso. La otra forma es especificar un mapeo en la salida de `elasticsearch {}` . Eso es lo que se muestra aquí.

```
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
    }
  }
}
```

Esto salida `metrics` eventos a `metrics-` índices en Elasticsearch, que rotarán semanalmente usando la semana ISO. La plantilla utilizada para los nuevos índices se define como parte de esta configuración. Definir una plantilla tiene la ventaja de forzar los tipos de campos a un tipo uniforme. Esto es útil en configuraciones más grandes donde varios tipos pueden intentar definir un campo como un tipo de datos ligeramente diferente.

Este método es útil en entornos de prueba y control de calidad, ya que las plantillas de ElasticSearch están definidas por el código LogStash y no tienen que configurarse por separado como parte de la configuración del clúster de ElasticSearch.

Lea Empezando con logstash en línea: https://riptutorial.com/es/logstash/topic/6903/empezando-con-logstash

Creditos

S. No	Capítulos	Contributors
1	Empezando con logstash	Community, sysadmin1138