Бесплатная электронная книга

УЧУСЬ

logstash

Free unaffiliated eBook created from
Stack Overflow contributors.

#logstash

Около

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

глава 1: Начало работы с logstash

замечания

В этом разделе представлен обзор того, что такое logstash, и почему разработчик может захотеть его использовать.

Следует также упомянуть любые крупные темы в логсташе и ссылки на связанные темы. Поскольку документация для logstash новая, вам может потребоваться создать начальные версии этих связанных тем.

Examples

Установка или настройка

Подробные инструкции по настройке или установке логсташа.

Основной, полный пример Syslog

Исходя из своих корней, Logstash имеет возможность анализировать и хранить данные syslog. В этом примере показана базовая конфигурация, которая поможет вам в этом.

```
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"
    ]
  }
}
```

Вывод на ElasticSearch: несколько индексов и отображений

Иногда вам нужно выводить на несколько индексов в ElasticSearch или иметь настраиваемое сопоставление, которое вы хотите применить к новым индексам по мере их перемещения.

Существует два способа применения настраиваемого сопоставления. Один из способов - загрузить шаблон ElasticSearch. Для этого обратитесь к документации ElasticSearch. Другой способ - указать отображение в самом выходе `elasticsearch {}` . Вот что показано здесь.

```
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
    }
  }
}
```

Это приведет к `metrics-` событий `metrics` в `metrics-` индексы на ElasticSearch, которые будут вращаться еженедельно с использованием недели ISO. Шаблон, используемый для новых индексов, определяется как часть этой конфигурации. Преимущество шаблона состоит в том, чтобы форматировать типы полей в единый тип. Это полезно в более крупных конфигурациях, где несколько типов могут пытаться определить поле в виде немного другого типа данных.

Этот метод полезен для промежуточных и QA-сред, поскольку шаблоны ElasticSearch определяются кодом LogStash и не должны настраиваться отдельно как часть настройки кластера ElasticSearch.

Прочитайте Начало работы с logstash онлайн: https://riptutorial.com/ru/logstash/topic/6903/начало-работы-с-logstash

кредиты

S. No	Главы	Contributors
1	Начало работы с logstash	Community, sysadmin1138