EBook Gratuito

APPRENDIMENTO logstash

Free unaffiliated eBook created from
Stack Overflow contributors.

#logstash

Sommario

Di

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

Capitolo 1: Iniziare con il logstash

Osservazioni

Questa sezione fornisce una panoramica su cosa è il logstash e sul motivo per cui uno sviluppatore potrebbe volerlo utilizzare.

Dovrebbe anche menzionare eventuali soggetti di grandi dimensioni all'interno di logstash e collegarsi agli argomenti correlati. Poiché la documentazione per logstash è nuova, potrebbe essere necessario creare versioni iniziali di tali argomenti correlati.

Examples

Installazione o configurazione

Istruzioni dettagliate su come installare o installare il logstash.

Un esempio Syslog completo e di base

Andando alle sue radici, Logstash ha la capacità di analizzare e memorizzare i dati syslog. Questo esempio mostra una configurazione di base che ti porta a questo.

```
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"
    ]
  }
}
```

Trasmissione a ElasticSearch: più indici e mappature

A volte, è necessario eseguire l'output su più di un indice in ElasticSearch oppure disporre di una mappatura personalizzata che si desidera applicare ai nuovi indici mentre si spostano.

Esistono due modi per applicare una mappatura personalizzata. Un modo è caricare un modello ElasticSearch. Vedi la documentazione di ElasticSearch per questo. L'altro modo è specificare una mappatura nell'output di `elasticsearch {}` stesso. Questo è ciò che è mostrato qui.

```
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
    }
  }
}
```

Ciò uscita `metrics` eventi per `metrics-` indici in elasticsearch, che ruoterà settimanale utilizzando settimana ISO. Il modello utilizzato per i nuovi indici è definito come parte di questa configurazione. La definizione di un modello ha il vantaggio di forzare i tipi di campi a un tipo uniforme. Ciò è utile in configurazioni più grandi in cui più tipi possono tentare di definire un campo come un tipo di dati leggermente diverso.

Questo metodo è utile negli ambienti di staging e QA, poiché i modelli ElasticSearch sono definiti dal codice LogStash e non devono essere configurati separatamente come parte dell'installazione del cluster ElasticSearch.

Leggi Iniziare con il logstash online: https://riptutorial.com/it/logstash/topic/6903/iniziare-con-il-logstash

Titoli di coda

S. No	Capitoli	Contributors
1	Iniziare con il logstash	Community, sysadmin1138