eBook Gratuit

APPRENEZ logstash

eBook gratuit non affilié créé à partir des **contributeurs de Stack Overflow.**

#logstash

Table des matières

À propos

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

Chapitre 1: Démarrer avec logstash

Remarques

Cette section fournit une vue d'ensemble de ce qu'est logstash et pourquoi un développeur peut vouloir l'utiliser.

Il devrait également mentionner tous les grands sujets dans logstash et établir un lien avec les sujets connexes. La documentation de logstash étant nouvelle, vous devrez peut-être créer des versions initiales de ces rubriques connexes.

Examples

Installation ou configuration

Instructions détaillées sur la configuration ou l'installation de logstash.

Un exemple Syslog de base complet

En allant à ses racines, Logstash a la capacité d'analyser et de stocker les données Syslog. Cet exemple montre une configuration de base qui vous mène à cela.

```
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"
    ]
  }
}
```

Sortie vers ElasticSearch: plusieurs indices et mappages

Parfois, vous devez générer plusieurs index dans ElasticSearch ou créer un mappage personnalisé à appliquer aux nouveaux index.

Il existe deux manières d'appliquer un mappage personnalisé. Une façon consiste à télécharger un modèle ElasticSearch. Voir la documentation ElasticSearch pour cela. L'autre façon consiste à spécifier un mappage dans la sortie `elasticsearch {}` elle-même. C'est ce qui est montré ici.

```
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
    }
  }
}
```

Cela sortie `metrics` événements `metrics-` index sur ElasticSearch, qui tournera à l' aide hebdomadaire la semaine ISO. Le modèle utilisé pour les nouveaux index est défini dans le cadre de cette configuration. La définition d'un modèle a l'avantage de forcer les types de champs à un type uniforme. Ceci est utile dans les configurations plus grandes où plusieurs types peuvent tenter de définir un champ comme un type de données légèrement différent.

Cette méthode est utile dans les environnements de transfert et d'assurance qualité, car les modèles ElasticSearch sont définis par le code LogStash et ne doivent pas être configurés séparément dans le cadre de la configuration du cluster ElasticSearch.

Lire Démarrer avec logstash en ligne: https://riptutorial.com/fr/logstash/topic/6903/demarrer-avec-logstash

Crédits

S. No	Chapitres	Contributeurs
1	Démarrer avec logstash	Community, sysadmin1138