**FileBeat安装配置文档**

V1.0.0

王智强 @ Enlink 数据中心

**目录**

[1. 概述 3](#_Toc22581)

[1.1. 说明 3](#_Toc10098)

[2. 安装条件 4](#_Toc27247)

[2.1. 安装环境 4](#_Toc29127)

[2.2. 配置文件 4](#_Toc901)

[2.3. 文件解压 5](#_Toc19691)

[2.4. 启动脚本程序 5](#_Toc21253)

[2.5. 配置文件修改 5](#_Toc16199)

[3. Filebeat操作命令 7](#_Toc20097)

[3.1. 启动关闭重启命令 7](#_Toc30147)

[3.2. 其它操作命令 7](#_Toc20057)

[4. 异常处理 8](#_Toc12789)

[4.1. Filebeat关闭异常 8](#_Toc30136)

# 概述

本章节描述Filebeat的安装和配置以及通用Filebeat指令。

## 说明

Filebeat是一款由elastic公司开发的轻量型日志采集器，Filebeat会监控日志目录或者指定的日志文件，追踪读取这些文件（追踪文件的变化），并且转发这些信息到elasticsearch或者logstarsh中存放。本文档详细介绍了Filebeat的安装与配置，请按照文档的说明和步骤进行操作。

# 安装条件

本章节描述Filebeat的安装环境与配置文件以及安装与配置步骤。

## 安装环境

本文安装环境为Linux CentOS系统（CentOS7.0以上），并且确认elasticsearch版本是否相对应（elasticsearch版本要求6.0以上，Filebeat与Elasticsearch没有特殊的安装顺序）。

检查Linux版本命令为：

|  |
| --- |
| cat /etc/redhat-release |

如图2-1所示红色方圈为当前Linux CentOS版本号（7.4）：



图 2-1 Linux版本号

检查elasticsearch是否配置完成命令为:

|  |
| --- |
| uname -a curl -XGET “localhost:9200” |

如下图2-2所示，出现相似输出结果则elasticsearch配置完成，红色方框为当前版本号（6.3.0）：

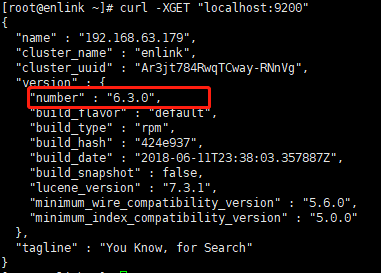


图 2-2 elasticsearch版本号

## 配置文件

本文档安装和配置Filebeat所需文件为:filebeat-casbs-v0.0.1.tar.gz压缩包。

## 文件解压

将准备的压缩包文件用如下命令解压：

|  |
| --- |
| tar zxvf filebeat-casbs-v0.0.1.tar.gz |

## 启动脚本程序

进入解压的文件夹内，使用命令：

|  |
| --- |
| sh ./install.sh |

脚本执行过程中会判断Filebeat是否安装，如若已安装则会提示是否覆盖安装，如图2-3所示：

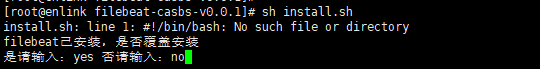


图 2-3 脚本提示

输入yes则开始覆盖安装，输入no或者其他命令则推出安装，具体事例如图2-4所示：

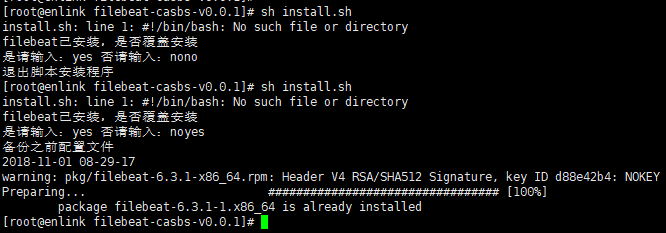


图 2-4 运行实例

完成以上步骤则配置完成。

## 配置文件修改

完成以上操作后，打开目录(/etc/filebeat)下的配置文件filebeat.yml，找到output.elasticsearch配置下的hosts属性，将要连接的服务器ip按如下格式添加（连接本机则ip默认为127.0.0.1）:

a.若只需要连接本机的elasticsearch则配置为：

|  |
| --- |
| hosts: ["127.0.0.1"] |

b.若需要连接本机和另一台服务器的elasticsearch则配置为（假设ip为192.168.63.177）：

|  |
| --- |
| hosts: ["127.0.0.1","192.168.63.177"] |

c.若需要连接另俩台服务器的elasticsearch则配置为（假设ip分别为192.168.63.177,192.168.63.179）：

|  |
| --- |
| hosts: ["192.168.63.177","192.168.63.179"] |

d.若需要连接另四台服务器的elasticsearch则配置为（假设ip分别为192.168.63.177,192.168.63.179,192.168.63.180,192.168.63.181）：

|  |
| --- |
| hosts: ["192.168.63.177","192.168.63.179","192.168.63.180","192.168.63.181"] |

# Filebeat操作命令

本章节描述Filebeat的启动关闭重启等操作命令。

## 启动关闭重启命令

启动命令 service filebeat start ，关闭命令 service filebeat stop， 重启命令 service filebeat restart 如下图3-1所示：

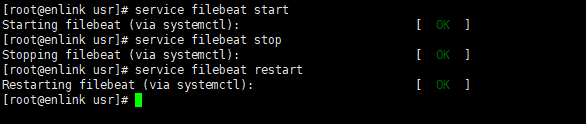


图 3-1 命令展示

## 其它操作命令

查看当前Filebeat版本命令 filebeat version ，测试配置设置命令 filebeat test config ，测试Filebeat测试当前设置连接和输出命令 filebeat test output 如下图3-2所示：

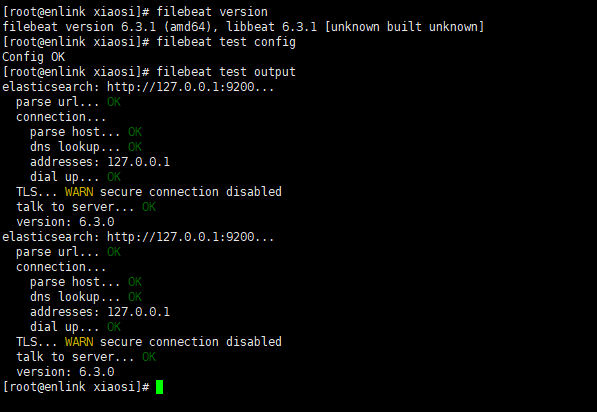


图 3-2 命令展示

# 异常处理

## Filebeat关闭异常

如遇到用service filebeat stop命令关闭Filebeat程序后，还有关于该程序的进程存在，则打开Filebeat日志查看（查看命令 ：tail -f /var/log/filebeat/filebeat），若有类似下表错误：

|  |
| --- |
| ERROR elasticsearch/elasticsearch.go:165 Error connecting to Elasticsearch at http://192.168.63.183:9200: Get http://192.168.63.183:9200: dial tcp 192.168.63.183:9200: connect: connection refused |

则需要检测Elasticsearch是否安装以及Filebeat连接Elasticsearch的ip是否准确，该进程在一段时间内会自动结束（5~10分钟）也可用kill命令强制清除。