**EFLK简易安装手册**

**一，概述**

**本文是一个以EFLF5.0版本为例的简易安装手册，EFLK5.0是本文成文时最新的版本，主要用于日志数据的提取、汇总、查询和分析；EFLK由四个部分组成：**

**（1）Filebeat 负责跟踪日志文件的更新、提取日志记录、发送给Logstash或者Elasticsearch。**

**（2）Logstash 负责汇总各种数据源发送过来的数据，并转发给Elasticsearch。**

**（3）Elasticsearch 一个轻量级的全文搜索引擎，提供各种查询和分析接口。**

**（4）Kibana 为Elasticsearch提供一个WEB查询界面。**

**二，场景**

**在EFLK的应用场景中，服务器一般分为两种角色：**

**（1）查询服务器 （Service） 安装了 Eleasticsearch 和 Kibana 提供日志查询和分析服务。**

**（2）转发器（Forward）安装了 Logstash 汇总各种日志数据源的数据，并发送给查询服务器。**

**（3）日志数据源 （Data Source） 安装了 Filebeat 跟踪日志文件的更新，并将日志数据发送给 查询服务器 或者 转发器。**

**Logstash 可以搜集 Filebeat 发送来的数据，也可以搜集其他数据源发送过来的数据；同样，如果日志数据源只有 Filebeat，也可以跳过 Logstash 直接将数据发给 Eleasticsearch。**

**下面我们用真实场景中的例子，来详细讲解EFLK的安装步骤。真实场景中有三台服务器，其中两台在生产环境中为外界提供WEB服务，是日志数据的主要来源；另外一台则搜集日志数据，并对内网用户提供日志查询分析功能。三台机器的IP及功能如下：**

**（1）10.1.51.56 生产环境WEB前置机1 & 日志数据源**

**（2）10.1.51.57 生产环境WEB前置机2 & 日志数据源**

**（3）10.1.51.58 日志转发器 & 日志查询服务器**

**三，安装步骤**

**（1）安装依赖软件包**

sudo yum install java-1.8.0-openjdk

sudo yum install ruby rubygems

sudo gem install bundler

**（2）安装YUM源**

**#安装官方YUM源**

sudo rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

cd /etc/yum.repos.d/

sudo vim logstash.repo

~~~~~~~~~~~~~~~~

[logstash-5.x]

name=Elastic repository for 5.x packages

baseurl=https://artifacts.elastic.co/packages/5.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

~~~~~~~~~~~~~~~~

**#安装国内镜像YUM源（如果官方源太慢可以考虑这个）**

cd /etc/yum.repos.d/

sudo vim logstash.repo

~~~~~~~~~~~~~~~~

[logstash]

name=elk

baseurl=https://mirror.tuna.tsinghua.edu.cn/elasticstack/yum/elastic-5.x/

gpgcheck=0

enabled=1

~~~~~~~~~~~~~~~~

**（3）在10.1.51.58上安装 Logstash**

sudo yum install logstash

sudo vim /etc/logstash/conf.d/logstash.conf

~~~~~~~~~~~~~~~~

input {

stdin {}

}

output {

stdout {}

}

~~~~~~~~~~~~~~~~

**#测试功能（在系统终端手工输入日志内容，查看是否在系统终端输出）**

sudo /usr/share/logstash/bin/logstash --path.settings=/etc/logstash/

**#安装系统服务**

sudo /usr/share/logstash/bin/system-install

sudo initctl start logstash | sudo initctl stop logstash

**（4）在10.1.51.58上安装 Elasticsearch**

**#用YUM安装**

sudo yum install elasticsearch

**#用RPM包安装（如果安装YUM源失败，则可以直接在这RPM包）**

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.0.0.rpm

sudo rpm -vi elasticsearch-5.0.0.rpm

sudo chkconfig --add elasticsearch

**#测试功能**

sudo service elasticsearch start

curl http://localhost:9200/

**#配置Logstash**

sudo vim /etc/logstash/conf.d/logstash.conf

~~~~~~~~~~~~~~~~

input {

stdin {}

}

output {

elasticsearch {

hosts => [ "localhost:9200" ]

}

}

~~~~~~~~~~~~~~~~

**#测试Logstash和Elasticsearch协同工作情况（在系统终端手工输入日志内容，查看是否在curl命令中输出）**

sudo /usr/share/logstash/bin/logstash --path.settings=/etc/logstash/

curl -XGET 'localhost:9200/logstash/\_search?pretty&q=response=200'

**（5）在10.1.51.58上安装 Kibana**

**#用YUM安装**

sudo yum install kibana

**#用RPM包安装（如果安装YUM源失败，则可以直接在这RPM包）**

wget https://artifacts.elastic.co/downloads/kibana/kibana-5.0.0-x86\_64.rpm

sudo rpm -vi kibana-5.0.0-x86\_64.rpm

**#修改配置文件**

sudo vim /etc/kibana/kibana.yml

~~~~~~~~~~~~~~~~

server.host: "10.1.51.58"

server.name: "test.kibana.com"

elasticsearch.url: "http://localhost:9200"

~~~~~~~~~~~~~~~~

**#启动Kibana**

sudo /etc/init.d/kibana start

**#在客户端配置HOSTS（并打开浏览器，访问http://test.kibana.com）**

10.1.51.58 test.kibana.com

**（6）在10.1.51.56/57上安装 Filebeat**

**#用YUM安装**

sudo yum install filebeat

**#用RPM包安装（如果安装YUM源失败，则可以直接在这RPM包）**

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.0.0-x86\_64.rpm

sudo rpm -vi filebeat-5.0.0-x86\_64.rpm

**#修改配置文件**

sudo vim /etc/filebeat/filebeat.yml

~~~~~~~~~~~~~~~~

filebeat.prospectors:

- input\_type: log

paths:

- /opt/logs/[www.cp.com-access\_log](http://www.cp.com-access_log)

- /opt/logs/[www.cp.com-error\_log](http://www.cp.com-error_log)

- /opt/logs/php-error\_log

output.logstash:

hosts: ["10.1.51.58:5043"]

~~~~~~~~~~~~~~~~

**#修改10.1.51.58上Logstash的配置文件**

sudo vim /etc/logstash/conf.d/logstash.conf

~~~~~~~~~~~~~~~~

input {

beats {

port => "5043"

}

}

output {

elasticsearch {

hosts => [ "localhost:9200" ]

}

}

~~~~~~~~~~~~~~~~

**#启动Filebeat**

sudo /etc/init.d/filebeat start

**#或者**

sudo nohup /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml >/dev/null 2>&1 &

**四，后记**

**本文是一个极为简易的安装手册，没有任何的图表，屏幕截图；因为随着时间的推移，技术的演进；今天看似事无巨细且言之凿凿的文字，却可能对后来的读者造成巨大的困惑；但只要严格按照本文的指导进行操作，还是可以完成EFLK5.0版本的安装和配置操作。至于更多的细节，希望读者抱着探索的精神不断的探究和完善。希望本文可以在实用性的角度帮助读者解决燃眉之急，并为读者开启一扇探索之门。**

**2016-11-14 15:55 北京 太阳宫 彣骢彦骐**