[Edit](http://maxiang.info/#/?provider=evernote&guid=77af9f81-ffd6-4117-b50e-12b7a8d6b9aa&notebook=linux)

# ELK 日志收集与分析

linux ELK

## elk 介绍

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is released as open source under the terms of the Apache License. Elasticsearch is the most popular enterprise search engine followed by Apache Solr, also based on Lucene.

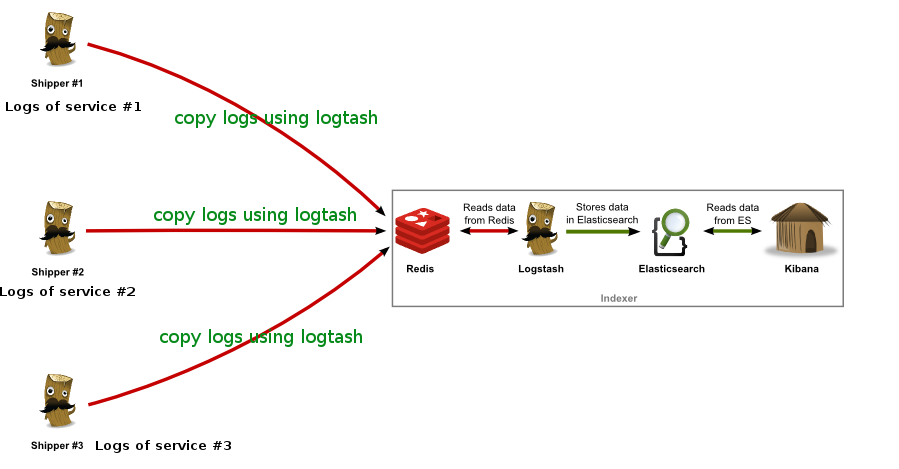
Kibana is an open source data visualization plugin for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data

Logstash is a tool for managing events and logs. When used generically the term encompases a larger system of log collection, processing, storage and searching activities.

elk 官网 <https://www.elastic.co>

日志是运维的一只眼，这里用ELK仅用于收集日志并展示，不进行深入探讨

首先来看看ELK架构



## ELK 安装

安装官网有，下载RPM包最为方便，以下安装方式仅供参考

elasticsearch安装

下载并安装GPG key

[root@hadoop-node1 ~]# rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

添加yum仓库

[root@hadoop-node1 ~]# vim /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-2.x]

name=Elasticsearch repository **for** 2.x packages

baseurl=http://packages.elastic.co/elasticsearch/2.x/centos

gpgcheck=1

gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch

enabled=1

安装elasticsearch

[root@hadoop-node1 ~]# yum install -y elasticsearch

#logstash安装

#添加yum仓库

[root@hadoop-node2 ~]# vim /etc/yum.repos.d/logstash.repo

[logstash-2.1]

name=Logstash repository **for** 2.1.x packages

baseurl=http://packages.elastic.co/logstash/2.1/centos

gpgcheck=1

gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch

enabled=1

#安装logstash

[root@hadoop-node2 ~]# yum install -y logstash

#安装kibana

cd /usr/local/src

wget https://download.elastic.co/kibana/kibana/kibana-4.3.1-linux-x64.tar.gz

tar zxf kibana-4.3.1-linux-x64.tar.gz

[root@hadoop-node1 src]# mv kibana-4.3.1-linux-x64 /usr/local/

[root@hadoop-node1 src]# ln -s /usr/local/kibana-4.3.1-linux-x64/ /usr/local/kibana

## Elasticsearch

首先配置elasticsearch

$ grep '^[a-z]' /etc/elasticsearch/elasticsearch.yml

cluster.name: sandow

node.name: linux-node1

path.data: /data/es-data

path.logs: /var/log/elasticsearch/

bootstrap.mlockall: true

network.host: 0.0.0.0

http.port: 9200

discovery.zen.unicast.hosts: ["127.0.0.1",]

$ mkdir -p /data/es-data

$ chown -R elasticsearch:elasticsearch /data/es-data

$ systemctl start elasticsearch

$ curl 10.0.0.153:9200

{

"name" : "linux-node1",

"cluster\_name" : "oldboy",

"version" : {

"number" : "2.1.0",

"build\_hash" : "72cd1f1a3eee09505e036106146dc1949dc5dc87",

"build\_timestamp" : "2015-11-18T22:40:03Z",

"build\_snapshot" : false,

"lucene\_version" : "5.3.1"

},

"tagline" : "You Know, for Search"

}

这时便可以向elasticsearch增加索引咯

[root@docker elasticsearch]# curl -i -XGET 'http://10.0.0.153:9200/\_count?pretty' -d {'

"query": {

"match\_all" :{}}'

HTTP/1.1 200 OK

Content-Type: application/json; charset=UTF-8

Content-Length: 95

{

"count" : 0,

"\_shards" : {

"total" : 0,

"successful" : 0,

"failed" : 0

}

}

但是这里还需要再增加一些插件来查看索引

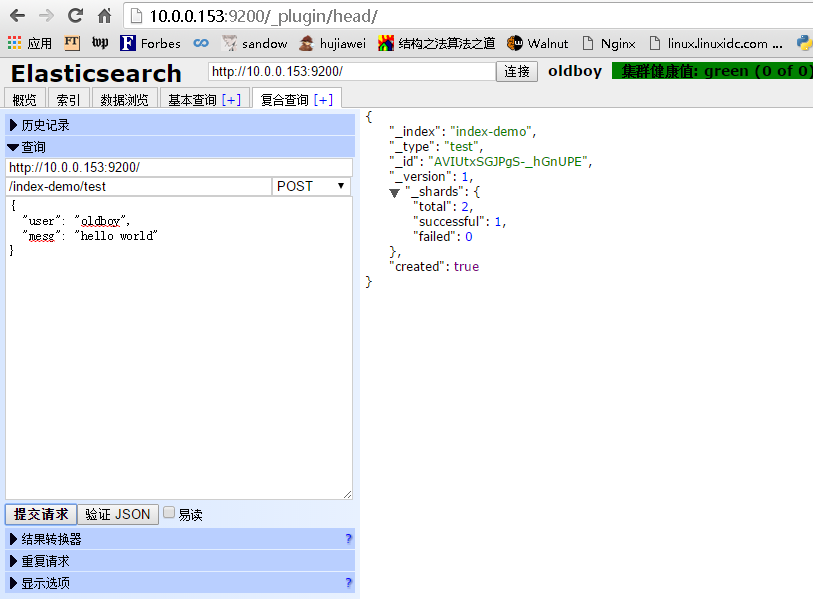
/usr/share/elasticsearch/bin/plugin **install** marvel-**agent**

/usr/**share**/elasticsearch/**bin**/**plugin** remove marvel-**agent**

/usr/**share**/elasticsearch/**bin**/**plugin** **install** mobz/elasticsearch-**head**

/usr/**share**/elasticsearch/**bin**/**plugin** **install** lmenezes/elasticsearch-kopf

head插件的访问地址为 <http://10.0.0.153:9200/_plugin/head>



head bigdesk kopf 1.centos7 es2.1 默认的组播发现无法发现 改成单播 2.bigdesk 不支持2.1

## logstach 使用方法

logstash 由三部门组成input,output filter。其功能就是收集，过滤，输出。

[root@linux-node1 ~]# /opt/logstash/bin/logstash -e 'input { stdin{} } output { stdout{} }'

[root@docker logstash]# /opt/logstash/bin/logstash -e 'input { stdin{} } output { stdout{ codec => rubydebug} }'

Settings: Default filter workers: 1

Logstash startup completed

hehe

{

"message" => "hehe",

"@version" => "1",

"@timestamp" => "2016-01-09T04:06:02.808Z",

"host" => "0.0.0.0"

}

在生产中一搬我们会使用配置文件来进行收集日志

[root@docker ~]# cat file.conf

input {

file {

path => "/var/log/messages"

**type** => "system"

start\_position => "beginning"

}

file {

path => "/var/log/elasticsearch/oldboy.log"

**type** => "es-error"

start\_position => "beginning"

}

}

output {

**if** [**type**] == "system" {

elasticsearch {

hosts => ["10.0.0.153:9200"]

index => "system-%{+YYYY.MM.dd}"

}

}

**if** [**type**] == "es-error" {

elasticsearch {

hosts => ["10.0.0.153:9200"]

index => "es-error-%{+YYYY.MM.dd}"

}

}

}

$ /opt/logstash/bin/logstash -f ~/file.conf

<https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html>

下面是生产中所使用的配置文件仅做举例

input{

file {

path => ["/srv/loginlog/login\_log\*", "/var/log/ytadmin/login\_log-\*"]

start\_position => "beginning"

**type** => "login"

}

file {

path => ["/usr/local/tomcat/logs/ssoserver.log","/usr/local/tomcat/logs/backadmin.log", "/usr/local/tomcat/logs/mallserver.log", "/usr/local/tomcat/logs/yxtserver.log"]

start\_position => "beginning"

**type** => "java\_log"

codec => multiline {

pattern => "^\["

negate => true

what => "previous"

}

}

}

filter {

**if** [**type**] == "login" {

grok {

**match** => { "message" => "%{LOGINLOG}"

}

}

}

geoip {

source => "client\_ip"

add\_tag => "[geoip]"

}

}

output {

**if** [**type**] == "java\_log" {

redis{

host => "10.51.48.249"

port => "6379"

db => "6"

data\_type => "list"

key => "java\_log"

password => "f7ypY/JwjAI9MQ=="

}

}

**if** [**type**] == "login" {

redis{

host => "10.51.48.249"

port => "6379"

db => "6"

data\_type => "list"

key => "login"

password => "f7ypY/JwjAI9MQ=="

}

}

}

====================

input{

redis {

**type** => "nginx\_ytadmin\_log"

host => "10.51.48.249"

db => "6"

key => "nginx\_ytadmin\_log"

password => "f7ypY/JwjAI9MQ=="

data\_type => "list"

}

}

output {

**if** [**type**] == "nginx\_ytadmin\_log" {

elasticsearch {

hosts => "127.0.0.1"

index => "logstash-nginx\_ytadmin\_log-%{+YYY.MM.dd}"

}

}

}

以上为收集JAVA 日志，nginx日志的配置文件，其中grok是是自定义的，所以需要放到**/opt/logstash/patterns/** 下面没有就需要新建，文件名字可以随便起，但最限可以自己认得

$ cat /opt/logstash/patterns/nginx

NGINXACCESS %{IPORHOST:client\_ip} (%{USER:ident}|-) (%{USER:auth}|-) \[%{HTTPDATE:timestamp}\] \"(?:%{WORD:verb} (%{NOTSPACE:request}|-)(?: HTTP/%{NUMBER:http\_version})?|-)\" (%{NUMBER:response}|-) (?:%{NUMBER:bytes}|-) \"(%{NOTSPACE:referrer}|-)\" \"%{GREEDYDATA:agent}\" \"(%{IPV4:x\_forword}|-)\" (%{BASE16FLOAT:request\_time}|-) (%{BASE16FLOAT:upstream\_response\_time}|-)

LOGINLOG .\***value** \('%{BASE10NUM:userid}','(%{BASE10NUM:gameid}|null)','(%{HOSTNAME:agent}|null)','(%{USERNAME:imeil}|null|)','(%{BASE10NUM:device}|null)','(%{BASE10NUM:login\_time}|null)','(%{BASE10NUM:reg\_time}|null)','(%{BASE10NUM:fromflag}|null)','(?:%{IPORHOST:agent\_ip}|null)'\);

NGINXACCESS 与nginx.conf里的main日志格式必须一致下面是nginx.conf里的配置

**log\_format** main '$remote\_addr - $remote\_user [$time\_local] "$request" '

'$status $body\_bytes\_sent "$http\_referer" '

'"$http\_user\_agent" "$http\_x\_forwarded\_for" $request\_time $upstream\_response\_time';

## kibana 展示

展示仅是鼠标手，不能记下来，好苦脑，来个配置吧

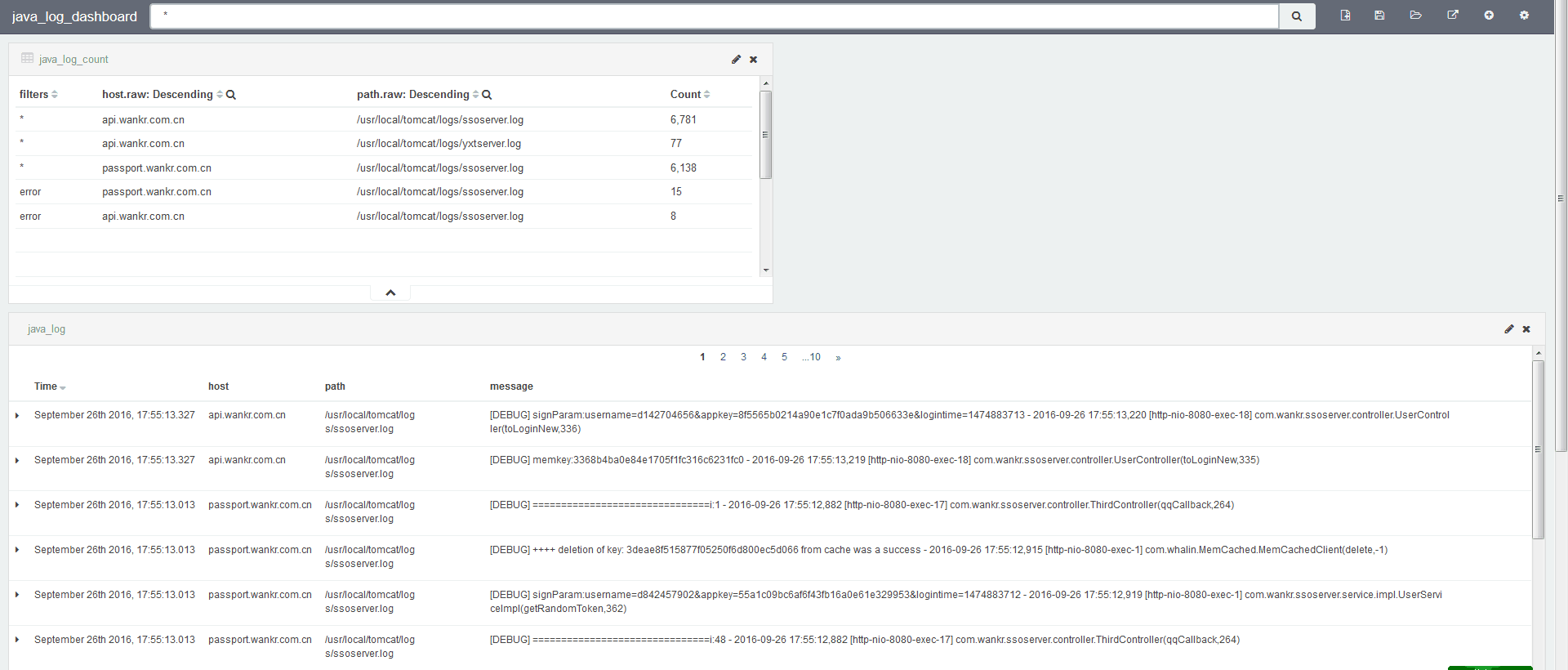
[root@localhost /usr/local/kibana]# grep '^[a-Z]' config/kibana.yml

server.port: 5601

server.host: "0.0.0.0"

elasticsearch.url: "http://192.168.1.127:9200"

kibana.index: ".kibana"



生产如何上线ELK

1. 日志分类

系统日志 rsyslog logstash syslog 插件

访问日志 nginx logstach codec json

错误日志 file logstash file + mulitline

运行日志 file logstash codec json

设备日志 syslog logstach syslog 插件

debug日志 file logstach json or mulitline

1. 日志标准化

路径 固定

格式 尽量json

1. 从系统日志开始收集，>> 错误日志，>> 运行日志， >> 访问日志

目前使用superviser来做进程的管理是非常明智的，

pip install supervisor

看几个文件

[root@localhost /etc/logstash/conf.d]# egrep -v "^;|^$" /etc/supervisord.conf

[unix\_http\_server]

file=/tmp/supervisor.sock ; (the path to the socket file)

[supervisord]

logfile=/tmp/supervisord.log ; (main log file;default $CWD/supervisord.log)

logfile\_maxbytes=50MB ; (max main logfile bytes b4 rotation;default 50MB)

logfile\_backups=10 ; (num **of** main logfile rotation backups;default 10)

loglevel=info ; (log level;default info; others: debug,warn,trace)

pidfile=/tmp/supervisord.pid ; (supervisord pidfile;default supervisord.pid)

nodaemon=false ; (start in foreground **if** true;default false)

minfds=1024 ; (min. avail startup file descriptors;default 1024)

minprocs=200 ; (min. avail process descriptors;default 200)

[rpcinterface:supervisor]

supervisor.rpcinterface\_factory = supervisor.rpcinterface:make\_main\_rpcinterface

[supervisorctl]

serverurl=unix:///tmp/supervisor.sock ; use a unix:// URL for a unix socket

[include]

files = /etc/supervisor/\*.conf

[root@localhost /etc/supervisor]# cat kibana.conf

[program:kibana]

directory = /usr/local/kibana/bin/ ; 程序的启动目录

command = /usr/local/kibana/bin/kibana ; 启动命令，可以看出与手动在命令行启动的命令是一样的

autostart = true ; 在 supervisord 启动的时候也自动启动

startsecs = 5 ; 启动 5 秒后没有异常退出，就当作已经正常启动了

autorestart = true ; 程序异常退出后自动重启

startretries = 3 ; 启动失败自动重试次数，默认是 3

user = root ; 用哪个用户启动

redirect\_stderr = true ; 把 stderr 重定向到 stdout，默认 false

stdout\_logfile\_maxbytes = 20MB ; stdout 日志文件大小，默认 50MB

stdout\_logfile\_backups = 20 ; stdout 日志文件备份数

; stdout 日志文件，需要注意当指定目录不存在时无法正常启动，所以需要手动创建目录（supervisord 会自动创建日志文件）

stdout\_logfile = /var/log/supervisor/kibana.log

[root@localhost /etc/supervisor]# cat logstash.conf

[program:logstash]

command = /opt/logstash/bin/logstash agent --config /etc/logstash/conf.d/ --log /var/log/logstash/logstash.log

numprocs = 1

autostart = true ; 在 supervisord 启动的时候也自动启动

startsecs = 5 ; 启动 5 秒后没有异常退出，就当作已经正常启动了

autorestart = true ; 程序异常退出后自动重启

startretries = 3 ; 启动失败自动重试次数，默认是 3

#user = root ; 用哪个用户启动

#redirect\_stderr = true ; 把 stderr 重定向到 stdout，默认 false

#stdout\_logfile\_maxbytes = 20MB ; stdout 日志文件大小，默认 50MB

#stdout\_logfile\_backups = 20 ; stdout 日志文件备份数

#stdout\_logfile = /var/log/supervisor/logstash.log

搞定，这样elk就完成咯。

%23%20ELK%20%u65E5%u5FD7%u6536%u96C6%u4E0E%u5206%u6790%0A@%28linux%29%5BELK%5D%0A%0A%0A%23%23%20elk%20%u4ECB%u7ECD%0AElasticsearch%20is%20a%20search%20engine%20based%20on%20Lucene.%20It%20provides%20a%20distributed%2C%20multitenant-capable%20full-text%20search%20engine%20with%20an%20HTTP%20web%20interface%20and%20schema-free%20JSON%20documents.%20Elasticsearch%20is%20developed%20in%20Java%20and%20is%20released%20as%20open%20source%20under%20the%20terms%20of%20the%20Apache%20License.%20Elasticsearch%20is%20the%20most%20popular%20enterprise%20search%20engine%20followed%20by%20Apache%20Solr%2C%20also%20based%20on%20Lucene.%0A%0A%20Kibana%20is%20an%20open%20source%20data%20visualization%20plugin%20for%20Elasticsearch.%20It%20provides%20visualization%20capabilities%20on%20top%20of%20the%20content%20indexed%20on%20an%20Elasticsearch%20cluster.%20Users%20can%20create%20bar%2C%20line%20and%20scatter%20plots%2C%20or%20pie%20charts%20and%20maps%20on%20top%20of%20large%20volumes%20of%20data%0A%0ALogstash%20is%20a%20tool%20for%20managing%20events%20and%20logs.%20When%20used%20generically%20the%20term%20encompases%20a%20larger%20system%20of%20log%20collection%2C%20processing%2C%20storage%20and%20searching%20activities.%0A%0Aelk%20%u5B98%u7F51%20https%3A//www.elastic.co%0A%0A%u65E5%u5FD7%u662F%u8FD0%u7EF4%u7684%u4E00%u53EA%u773C%uFF0C%u8FD9%u91CC%u7528ELK%u4EC5%u7528%u4E8E%u6536%u96C6%u65E5%u5FD7%u5E76%u5C55%u793A%uFF0C%u4E0D%u8FDB%u884C%u6DF1%u5165%u63A2%u8BA8%0A%u9996%u5148%u6765%u770B%u770BELK%u67B6%u6784%0A%21%5BAlt%20text%5D%28./1474880624382.png%29%0A%0A%0A%0A%23%23%20ELK%20%u5B89%u88C5%20%0A%u5B89%u88C5%u5B98%u7F51%u6709%uFF0C%u4E0B%u8F7DRPM%u5305%u6700%u4E3A%u65B9%u4FBF%uFF0C%u4EE5%u4E0B%u5B89%u88C5%u65B9%u5F0F%u4EC5%u4F9B%u53C2%u8003%0Aelasticsearch%u5B89%u88C5%0A%60%60%60%0A%u4E0B%u8F7D%u5E76%u5B89%u88C5GPG%20key%0A%5Broot@hadoop-node1%20%7E%5D%23%20rpm%20--import%20https%3A//packages.elastic.co/GPG-KEY-elasticsearch%0A%0A%u6DFB%u52A0yum%u4ED3%u5E93%0A%5Broot@hadoop-node1%20%7E%5D%23%20vim%20/etc/yum.repos.d/elasticsearch.repo%0A%5Belasticsearch-2.x%5D%0Aname%3DElasticsearch%20repository%20for%202.x%20packages%0Abaseurl%3Dhttp%3A//packages.elastic.co/elasticsearch/2.x/centos%0Agpgcheck%3D1%0Agpgkey%3Dhttp%3A//packages.elastic.co/GPG-KEY-elasticsearch%0Aenabled%3D1%0A%0A%u5B89%u88C5elasticsearch%0A%5Broot@hadoop-node1%20%7E%5D%23%20yum%20install%20-y%20elasticsearch%0A%0A%23logstash%u5B89%u88C5%0A%23%u6DFB%u52A0yum%u4ED3%u5E93%0A%5Broot@hadoop-node2%20%7E%5D%23%20vim%20/etc/yum.repos.d/logstash.repo%0A%5Blogstash-2.1%5D%0Aname%3DLogstash%20repository%20for%202.1.x%20packages%0Abaseurl%3Dhttp%3A//packages.elastic.co/logstash/2.1/centos%0Agpgcheck%3D1%0Agpgkey%3Dhttp%3A//packages.elastic.co/GPG-KEY-elasticsearch%0Aenabled%3D1%0A%0A%23%u5B89%u88C5logstash%0A%5Broot@hadoop-node2%20%7E%5D%23%20yum%20install%20-y%20logstash%0A%0A%23%u5B89%u88C5kibana%0A%0Acd%20/usr/local/src%0Awget%20https%3A//download.elastic.co/kibana/kibana/kibana-4.3.1-linux-x64.tar.gz%0Atar%20zxf%20kibana-4.3.1-linux-x64.tar.gz%0A%5Broot@hadoop-node1%20src%5D%23%20mv%20kibana-4.3.1-linux-x64%20/usr/local/%0A%5Broot@hadoop-node1%20src%5D%23%20ln%20-s%20/usr/local/kibana-4.3.1-linux-x64/%20/usr/local/kibana%0A%0A%60%60%60%0A%0A%23%23%20Elasticsearch%0A%u9996%u5148%u914D%u7F6Eelasticsearch%0A%60%60%60%0A%24%20grep%20%27%5E%5Ba-z%5D%27%20/etc/elasticsearch/elasticsearch.yml%20%0Acluster.name%3A%20sandow%0Anode.name%3A%20%20linux-node1%0Apath.data%3A%20/data/es-data%0Apath.logs%3A%20/var/log/elasticsearch/%0Abootstrap.mlockall%3A%20true%0Anetwork.host%3A%20%200.0.0.0%0Ahttp.port%3A%209200%0Adiscovery.zen.unicast.hosts%3A%20%5B%22127.0.0.1%22%2C%5D%0A%0A%24%20mkdir%20-p%20/data/es-data%0A%24%20chown%20%20-R%20elasticsearch%3Aelasticsearch%20/data/es-data%0A%24%20systemctl%20start%20elasticsearch%0A%0A%24%20curl%2010.0.0.153%3A9200%0A%7B%0A%20%20%22name%22%20%3A%20%22linux-node1%22%2C%0A%20%20%22cluster\_name%22%20%3A%20%22oldboy%22%2C%0A%20%20%22version%22%20%3A%20%7B%0A%20%20%20%20%22number%22%20%3A%20%222.1.0%22%2C%0A%20%20%20%20%22build\_hash%22%20%3A%20%2272cd1f1a3eee09505e036106146dc1949dc5dc87%22%2C%0A%20%20%20%20%22build\_timestamp%22%20%3A%20%222015-11-18T22%3A40%3A03Z%22%2C%0A%20%20%20%20%22build\_snapshot%22%20%3A%20false%2C%0A%20%20%20%20%22lucene\_version%22%20%3A%20%225.3.1%22%0A%20%20%7D%2C%0A%20%20%22tagline%22%20%3A%20%22You%20Know%2C%20for%20Search%22%0A%7D%0A%60%60%60%0A%u8FD9%u65F6%u4FBF%u53EF%u4EE5%u5411elasticsearch%u589E%u52A0%u7D22%u5F15%u54AF%0A%0A%60%60%60%0A%5Broot@docker%20elasticsearch%5D%23%20curl%20-i%20-XGET%20%27http%3A//10.0.0.153%3A9200/\_count%3Fpretty%27%20-d%20%7B%27%0A%22query%22%3A%20%7B%20%0A%20%20%20%20%22match\_all%22%20%3A%7B%7D%7D%27%0AHTTP/1.1%20200%20OK%0AContent-Type%3A%20application/json%3B%20charset%3DUTF-8%0AContent-Length%3A%2095%0A%0A%7B%0A%20%20%22count%22%20%3A%200%2C%0A%20%20%22\_shards%22%20%3A%20%7B%0A%20%20%20%20%22total%22%20%3A%200%2C%0A%20%20%20%20%22successful%22%20%3A%200%2C%0A%20%20%20%20%22failed%22%20%3A%200%0A%20%20%7D%0A%7D%0A%60%60%60%0A%0A%u4F46%u662F%u8FD9%u91CC%u8FD8%u9700%u8981%u518D%u589E%u52A0%u4E00%u4E9B%u63D2%u4EF6%u6765%u67E5%u770B%u7D22%u5F15%0A%60%60%60%0A/usr/share/elasticsearch/bin/plugin%20install%20marvel-agent%0A/usr/share/elasticsearch/bin/plugin%20remove%20%20marvel-agent%0A/usr/share/elasticsearch/bin/plugin%20install%20mobz/elasticsearch-head%0A/usr/share/elasticsearch/bin/plugin%20install%20lmenezes/elasticsearch-kopf%0A%60%60%60%0A%0Ahead%u63D2%u4EF6%u7684%u8BBF%u95EE%u5730%u5740%u4E3A%20%20http%3A//10.0.0.153%3A9200/\_plugin/head%0A%0A%21%5BAlt%20text%5D%28./1452307934909.png%29%0A%0A%0Ahead%20%20%20bigdesk%20%20kopf%20%20%201.centos7%20%20es2.1%20%20%u9ED8%u8BA4%u7684%u7EC4%u64AD%u53D1%u73B0%u65E0%u6CD5%u53D1%u73B0%20%20%u6539%u6210%u5355%u64AD%20%20%202.bigdesk%20%u4E0D%u652F%u63012.1%0A%0A%0A%0A%23%23logstach%20%u4F7F%u7528%u65B9%u6CD5%0Alogstash%20%u7531%u4E09%u90E8%u95E8%u7EC4%u6210input%2Coutput%20filter%u3002%u5176%u529F%u80FD%u5C31%u662F%u6536%u96C6%uFF0C%u8FC7%u6EE4%uFF0C%u8F93%u51FA%u3002%0A%0A%60%60%60%0A%5Broot@linux-node1%20%7E%5D%23%20/opt/logstash/bin/logstash%20-e%20%27input%20%7B%20stdin%7B%7D%20%7D%20output%20%7B%20stdout%7B%7D%20%7D%27%0A%0A%5Broot@docker%20logstash%5D%23%20/opt/logstash/bin/logstash%20-e%20%27input%20%7B%20stdin%7B%7D%20%7D%20output%20%7B%20stdout%7B%20codec%20%3D%3E%20rubydebug%7D%20%7D%27%0ASettings%3A%20Default%20filter%20workers%3A%201%0ALogstash%20startup%20completed%0Ahehe%0A%7B%0A%20%20%20%20%20%20%20%22message%22%20%3D%3E%20%22hehe%22%2C%0A%20%20%20%20%20%20%22@version%22%20%3D%3E%20%221%22%2C%0A%20%20%20%20%22@timestamp%22%20%3D%3E%20%222016-01-09T04%3A06%3A02.808Z%22%2C%0A%20%20%20%20%20%20%20%20%20%20%22host%22%20%3D%3E%20%220.0.0.0%22%0A%7D%0A%60%60%60%0A%0A%u5728%u751F%u4EA7%u4E2D%u4E00%u642C%u6211%u4EEC%u4F1A%u4F7F%u7528%u914D%u7F6E%u6587%u4EF6%u6765%u8FDB%u884C%u6536%u96C6%u65E5%u5FD7%0A%0A%60%60%60bash%0A%5Broot@docker%20%7E%5D%23%20cat%20file.conf%20%0Ainput%20%7B%0A%20%20%20%20file%20%7B%0A%20%20%20%20%20%20%20%20path%20%3D%3E%20%22/var/log/messages%22%0A%20%20%20%20%20%20%20%20type%20%3D%3E%20%22system%22%0A%20%20%20%20%20%20%20%20start\_position%20%3D%3E%20%22beginning%22%0A%20%20%20%20%7D%0A%20%20%20%20file%20%7B%0A%20%20%20%20%20%20%20%20path%20%3D%3E%20%22/var/log/elasticsearch/oldboy.log%22%0A%20%20%20%20%20%20%20%20type%20%3D%3E%20%22es-error%22%0A%20%20%20%20%20%20%20%20start\_position%20%3D%3E%20%22beginning%22%0A%20%20%20%20%7D%0A%0A%7D%0Aoutput%20%7B%0A%20%20%20%20if%20%5Btype%5D%20%3D%3D%20%22system%22%20%7B%0A%20%20%20%20%20%20%20%20elasticsearch%20%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20hosts%20%3D%3E%20%5B%2210.0.0.153%3A9200%22%5D%0A%20%20%20%20%20%20%20%20%20%20%20%20index%20%3D%3E%20%22system-%25%7B+YYYY.MM.dd%7D%22%0A%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%7D%0A%20%20%20%20if%20%5Btype%5D%20%3D%3D%20%22es-error%22%20%7B%0A%20%20%20%20%20%20%20%20elasticsearch%20%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20hosts%20%3D%3E%20%5B%2210.0.0.153%3A9200%22%5D%0A%20%20%20%20%20%20%20%20%20%20%20%20index%20%3D%3E%20%22es-error-%25%7B+YYYY.MM.dd%7D%22%0A%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%7D%0A%7D%0A%0A%24%20/opt/logstash/bin/logstash%20-f%20%7E/file.conf%20%0A%60%60%60%0A%0A%0A%0Ahttps%3A//www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html%0A%0A%u4E0B%u9762%u662F%u751F%u4EA7%u4E2D%u6240%u4F7F%u7528%u7684%u914D%u7F6E%u6587%u4EF6%u4EC5%u505A%u4E3E%u4F8B%0A%60%60%60%0Ainput%7B%0A%20%20%20%20file%20%7B%0A%20%20%20%20%20%20%20%20path%20%3D%3E%20%5B%22/srv/loginlog/login\_log\*%22%2C%20%22/var/log/ytadmin/login\_log-\*%22%5D%0A%20%20%20%20%20%20%20%20%20%20%20%20start\_position%20%3D%3E%20%22beginning%22%0A%20%20%20%20%20%20%20%20%20%20%20%20type%20%3D%3E%20%22login%22%0A%20%20%20%20%7D%0A%20%20%20%20file%20%7B%0A%20%20%20%20%20%20%20%20path%20%3D%3E%20%20%5B%22/usr/local/tomcat/logs/ssoserver.log%22%2C%22/usr/local/tomcat/logs/backadmin.log%22%2C%20%22/usr/local/tomcat/logs/mallserver.log%22%2C%20%22/usr/local/tomcat/logs/yxtserver.log%22%5D%0A%20%20%20%20%20%20%20%20%20%20%20%20start\_position%20%3D%3E%20%22beginning%22%0A%20%20%20%20%20%20%20%20%20%20%20%20type%20%3D%3E%20%22java\_log%22%0A%20%20%20%20%20%20%20%20%20%20%20%20codec%20%3D%3E%20multiline%20%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20pattern%20%3D%3E%20%22%5E%5C%5B%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20negate%20%3D%3E%20true%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20what%20%3D%3E%20%22previous%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%7D%0A%7D%0Afilter%20%7B%0A%20%20%20%20if%20%5Btype%5D%20%3D%3D%20%22login%22%20%7B%0A%20%20%20%20%20%20%20%20grok%20%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20match%20%3D%3E%20%7B%20%20%22message%22%20%3D%3E%20%20%22%25%7BLOGINLOG%7D%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%7D%20%20%0A%20%20%20%20%20geoip%20%7B%0A%20%20%20%20%20%20%20%20source%20%3D%3E%20%22client\_ip%22%0A%20%20%20%20%20%20%20%20add\_tag%20%3D%3E%20%22%5Bgeoip%5D%22%0A%20%20%20%20%20%20%20%20%20%20%7D%0A%7D%0Aoutput%20%7B%0A%20%20%20%20%20%20%20%20if%20%5Btype%5D%20%3D%3D%20%22java\_log%22%20%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20redis%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20host%20%3D%3E%20%2210.51.48.249%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20port%20%3D%3E%20%226379%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20db%20%3D%3E%20%226%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20data\_type%20%3D%3E%20%22list%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20key%20%3D%3E%20%22java\_log%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20password%20%3D%3E%20%22f7ypY/JwjAI9MQ%3D%3D%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20if%20%5Btype%5D%20%3D%3D%20%22login%22%20%7B%0A%20%20%20%20%20%20%20%20redis%7B%0A%20%20%20%20%20%20%20%20%20%20%20%20host%20%3D%3E%20%2210.51.48.249%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20port%20%3D%3E%20%226379%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20db%20%3D%3E%20%226%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20data\_type%20%3D%3E%20%22list%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20key%20%3D%3E%20%22login%22%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20password%20%3D%3E%20%22f7ypY/JwjAI9MQ%3D%3D%22%0A%20%20%20%20%20%20%20%20%7D%0A%20%20%20%20%7D%0A%7D%0A%0A%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%0Ainput%7B%0A%09redis%20%7B%0A%09%09type%20%3D%3E%20%22nginx\_ytadmin\_log%22%0A%09%09%09host%20%3D%3E%20%2210.51.48.249%22%0A%09%09%09db%20%3D%3E%20%226%22%0A%09%09%09key%20%3D%3E%20%22nginx\_ytadmin\_log%22%0A%09%09%09password%20%3D%3E%20%22f7ypY/JwjAI9MQ%3D%3D%22%0A%09%09%09data\_type%20%3D%3E%20%22list%22%0A%09%7D%0A%7D%0Aoutput%20%7B%0A%09if%20%5Btype%5D%20%3D%3D%20%22nginx\_ytadmin\_log%22%20%7B%0A%09%09elasticsearch%20%7B%0A%09%09%09hosts%20%3D%3E%20%22127.0.0.1%22%0A%09%09%09index%20%3D%3E%20%22logstash-nginx\_ytadmin\_log-%25%7B+YYY.MM.dd%7D%22%0A%09%09%7D%0A%20%20%20%20%7D%0A%7D%0A%60%60%60%0A%u4EE5%u4E0A%u4E3A%u6536%u96C6JAVA%09%u65E5%u5FD7%uFF0Cnginx%u65E5%u5FD7%u7684%u914D%u7F6E%u6587%u4EF6%uFF0C%u5176%u4E2Dgrok%u662F%u662F%u81EA%u5B9A%u4E49%u7684%uFF0C%u6240%u4EE5%u9700%u8981%u653E%u5230\*\*/opt/logstash/patterns/\*\*%20%u4E0B%u9762%u6CA1%u6709%u5C31%u9700%u8981%u65B0%u5EFA%uFF0C%u6587%u4EF6%u540D%u5B57%u53EF%u4EE5%u968F%u4FBF%u8D77%uFF0C%u4F46%u6700%u9650%u53EF%u4EE5%u81EA%u5DF1%u8BA4%u5F97%0A%60%60%60%0A%24%20cat%20/opt/logstash/patterns/nginx%0ANGINXACCESS%20%25%7BIPORHOST%3Aclient\_ip%7D%20%28%25%7BUSER%3Aident%7D%7C-%29%20%28%25%7BUSER%3Aauth%7D%7C-%29%20%5C%5B%25%7BHTTPDATE%3Atimestamp%7D%5C%5D%20%5C%22%28%3F%3A%25%7BWORD%3Averb%7D%20%28%25%7BNOTSPACE%3Arequest%7D%7C-%29%28%3F%3A%20HTTP/%25%7BNUMBER%3Ahttp\_version%7D%29%3F%7C-%29%5C%22%20%28%25%7BNUMBER%3Aresponse%7D%7C-%29%20%28%3F%3A%25%7BNUMBER%3Abytes%7D%7C-%29%20%5C%22%28%25%7BNOTSPACE%3Areferrer%7D%7C-%29%5C%22%20%5C%22%25%7BGREEDYDATA%3Aagent%7D%5C%22%20%5C%22%28%25%7BIPV4%3Ax\_forword%7D%7C-%29%5C%22%20%28%25%7BBASE16FLOAT%3Arequest\_time%7D%7C-%29%20%28%25%7BBASE16FLOAT%3Aupstream\_response\_time%7D%7C-%29%0ALOGINLOG%20.\*value%20%5C%28%27%25%7BBASE10NUM%3Auserid%7D%27%2C%27%28%25%7BBASE10NUM%3Agameid%7D%7Cnull%29%27%2C%27%28%25%7BHOSTNAME%3Aagent%7D%7Cnull%29%27%2C%27%28%25%7BUSERNAME%3Aimeil%7D%7Cnull%7C%29%27%2C%27%28%25%7BBASE10NUM%3Adevice%7D%7Cnull%29%27%2C%27%28%25%7BBASE10NUM%3Alogin\_time%7D%7Cnull%29%27%2C%27%28%25%7BBASE10NUM%3Areg\_time%7D%7Cnull%29%27%2C%27%28%25%7BBASE10NUM%3Afromflag%7D%7Cnull%29%27%2C%27%28%3F%3A%25%7BIPORHOST%3Aagent\_ip%7D%7Cnull%29%27%5C%29%3B%0A%60%60%60%0ANGINXACCESS%20%u4E0Enginx.conf%u91CC%u7684main%u65E5%u5FD7%u683C%u5F0F%u5FC5%u987B%u4E00%u81F4%u4E0B%u9762%u662Fnginx.conf%u91CC%u7684%u914D%u7F6E%0A%60%60%60%0A%20%20%20log\_format%20%20main%20%20%27%24remote\_addr%20-%20%24remote\_user%20%5B%24time\_local%5D%20%22%24request%22%20%27%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%27%24status%20%24body\_bytes\_sent%20%22%24http\_referer%22%20%27%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%27%22%24http\_user\_agent%22%20%22%24http\_x\_forwarded\_for%22%20%24request\_time%20%24upstream\_response\_time%27%3B%0A%60%60%60%0A%0A%23%23%20kibana%20%u5C55%u793A%0A%u5C55%u793A%u4EC5%u662F%u9F20%u6807%u624B%uFF0C%u4E0D%u80FD%u8BB0%u4E0B%u6765%uFF0C%u597D%u82E6%u8111%uFF0C%u6765%u4E2A%u914D%u7F6E%u5427%0A%60%60%60%0A%5Broot@localhost%20/usr/local/kibana%5D%23%20grep%20%27%5E%5Ba-Z%5D%27%20config/kibana.yml%20%20%20%20%20%20%20%0Aserver.port%3A%205601%0Aserver.host%3A%20%220.0.0.0%22%0Aelasticsearch.url%3A%20%22http%3A//192.168.1.127%3A9200%22%0Akibana.index%3A%20%22.kibana%22%0A%60%60%60%0A%0A%21%5BAlt%20text%5D%28./1474883898690.png%29%0A%0A%0A%0A%u751F%u4EA7%u5982%u4F55%u4E0A%u7EBFELK%0A%0A1.%20%u65E5%u5FD7%u5206%u7C7B%0A%20%20%u7CFB%u7EDF%u65E5%u5FD7%20%20rsyslog%20%20logstash%20syslog%20%u63D2%u4EF6%0A%20%20%u8BBF%u95EE%u65E5%u5FD7%20%20nginx%20%20%20logstach%20codec%20json%0A%20%20%u9519%u8BEF%u65E5%u5FD7%20%20file%20%20%20logstash%20file%20+%20mulitline%0A%20%20%u8FD0%u884C%u65E5%u5FD7%20%20file%20%20%20logstash%20codec%20json%0A%20%20%u8BBE%u5907%u65E5%u5FD7%20%20syslog%20%20logstach%20syslog%20%u63D2%u4EF6%0A%20%20debug%u65E5%u5FD7%20%20file%20%20logstach%20json%20or%20mulitline%0A%0A2.%20%u65E5%u5FD7%u6807%u51C6%u5316%0A%20%20%20%20%u8DEF%u5F84%20%u56FA%u5B9A%0A%20%20%20%20%u683C%u5F0F%20%u5C3D%u91CFjson%0A%20%20%20%20%0A3.%20%u4ECE%u7CFB%u7EDF%u65E5%u5FD7%u5F00%u59CB%u6536%u96C6%uFF0C%3E%3E%20%u9519%u8BEF%u65E5%u5FD7%uFF0C%3E%3E%20%u8FD0%u884C%u65E5%u5FD7%uFF0C%20%3E%3E%20%u8BBF%u95EE%u65E5%u5FD7%0A%0A%0A%u76EE%u524D%u4F7F%u7528superviser%u6765%u505A%u8FDB%u7A0B%u7684%u7BA1%u7406%u662F%u975E%u5E38%u660E%u667A%u7684%uFF0C%0A%0Apip%20install%20supervisor%0A%0A%u770B%u51E0%u4E2A%u6587%u4EF6%0A%60%60%60%0A%5Broot@localhost%20/etc/logstash/conf.d%5D%23%20egrep%20-v%20%22%5E%3B%7C%5E%24%22%20/etc/supervisord.conf%20%20%20%20%0A%5Bunix\_http\_server%5D%0Afile%3D/tmp/supervisor.sock%20%20%20%3B%20%28the%20path%20to%20the%20socket%20file%29%0A%5Bsupervisord%5D%0Alogfile%3D/tmp/supervisord.log%20%3B%20%28main%20log%20file%3Bdefault%20%24CWD/supervisord.log%29%0Alogfile\_maxbytes%3D50MB%20%20%20%20%20%20%20%20%3B%20%28max%20main%20logfile%20bytes%20b4%20rotation%3Bdefault%2050MB%29%0Alogfile\_backups%3D10%20%20%20%20%20%20%20%20%20%20%20%3B%20%28num%20of%20main%20logfile%20rotation%20backups%3Bdefault%2010%29%0Aloglevel%3Dinfo%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3B%20%28log%20level%3Bdefault%20info%3B%20others%3A%20debug%2Cwarn%2Ctrace%29%0Apidfile%3D/tmp/supervisord.pid%20%3B%20%28supervisord%20pidfile%3Bdefault%20supervisord.pid%29%0Anodaemon%3Dfalse%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3B%20%28start%20in%20foreground%20if%20true%3Bdefault%20false%29%0Aminfds%3D1024%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3B%20%28min.%20avail%20startup%20file%20descriptors%3Bdefault%201024%29%0Aminprocs%3D200%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3B%20%28min.%20avail%20process%20descriptors%3Bdefault%20200%29%0A%5Brpcinterface%3Asupervisor%5D%0Asupervisor.rpcinterface\_factory%20%3D%20supervisor.rpcinterface%3Amake\_main\_rpcinterface%0A%5Bsupervisorctl%5D%0Aserverurl%3Dunix%3A///tmp/supervisor.sock%20%3B%20use%20a%20unix%3A//%20URL%20%20for%20a%20unix%20socket%0A%5Binclude%5D%0Afiles%20%3D%20/etc/supervisor/\*.conf%0A%0A%5Broot@localhost%20/etc/supervisor%5D%23%20cat%20kibana.conf%20%0A%5Bprogram%3Akibana%5D%0Adirectory%20%3D%20/usr/local/kibana/bin/%20%3B%20%u7A0B%u5E8F%u7684%u542F%u52A8%u76EE%u5F55%0Acommand%20%3D%20/usr/local/kibana/bin/kibana%20%3B%20%u542F%u52A8%u547D%u4EE4%uFF0C%u53EF%u4EE5%u770B%u51FA%u4E0E%u624B%u52A8%u5728%u547D%u4EE4%u884C%u542F%u52A8%u7684%u547D%u4EE4%u662F%u4E00%u6837%u7684%0Aautostart%20%3D%20true%20%20%20%20%20%3B%20%u5728%20supervisord%20%u542F%u52A8%u7684%u65F6%u5019%u4E5F%u81EA%u52A8%u542F%u52A8%0Astartsecs%20%3D%205%20%20%20%20%20%20%20%20%3B%20%u542F%u52A8%205%20%u79D2%u540E%u6CA1%u6709%u5F02%u5E38%u9000%u51FA%uFF0C%u5C31%u5F53%u4F5C%u5DF2%u7ECF%u6B63%u5E38%u542F%u52A8%u4E86%0Aautorestart%20%3D%20true%20%20%20%3B%20%u7A0B%u5E8F%u5F02%u5E38%u9000%u51FA%u540E%u81EA%u52A8%u91CD%u542F%0Astartretries%20%3D%203%20%20%20%20%20%3B%20%u542F%u52A8%u5931%u8D25%u81EA%u52A8%u91CD%u8BD5%u6B21%u6570%uFF0C%u9ED8%u8BA4%u662F%203%0Auser%20%3D%20root%20%20%20%20%20%20%20%3B%20%u7528%u54EA%u4E2A%u7528%u6237%u542F%u52A8%0Aredirect\_stderr%20%3D%20true%20%20%3B%20%u628A%20stderr%20%u91CD%u5B9A%u5411%u5230%20stdout%uFF0C%u9ED8%u8BA4%20false%0Astdout\_logfile\_maxbytes%20%3D%2020MB%20%20%3B%20stdout%20%u65E5%u5FD7%u6587%u4EF6%u5927%u5C0F%uFF0C%u9ED8%u8BA4%2050MB%0Astdout\_logfile\_backups%20%3D%2020%20%20%20%20%20%3B%20stdout%20%u65E5%u5FD7%u6587%u4EF6%u5907%u4EFD%u6570%0A%3B%20stdout%20%u65E5%u5FD7%u6587%u4EF6%uFF0C%u9700%u8981%u6CE8%u610F%u5F53%u6307%u5B9A%u76EE%u5F55%u4E0D%u5B58%u5728%u65F6%u65E0%u6CD5%u6B63%u5E38%u542F%u52A8%uFF0C%u6240%u4EE5%u9700%u8981%u624B%u52A8%u521B%u5EFA%u76EE%u5F55%uFF08supervisord%20%u4F1A%u81EA%u52A8%u521B%u5EFA%u65E5%u5FD7%u6587%u4EF6%uFF09%0Astdout\_logfile%20%3D%20/var/log/supervisor/kibana.log%0A%5Broot@localhost%20/etc/supervisor%5D%23%20cat%20logstash.conf%20%0A%5Bprogram%3Alogstash%5D%0Acommand%20%3D%20/opt/logstash/bin/logstash%20agent%20--config%20/etc/logstash/conf.d/%20--log%20/var/log/logstash/logstash.log%20%0Anumprocs%20%3D%201%0Aautostart%20%3D%20true%20%20%20%20%20%3B%20%u5728%20supervisord%20%u542F%u52A8%u7684%u65F6%u5019%u4E5F%u81EA%u52A8%u542F%u52A8%0Astartsecs%20%3D%205%20%20%20%20%20%20%20%20%3B%20%u542F%u52A8%205%20%u79D2%u540E%u6CA1%u6709%u5F02%u5E38%u9000%u51FA%uFF0C%u5C31%u5F53%u4F5C%u5DF2%u7ECF%u6B63%u5E38%u542F%u52A8%u4E86%0Aautorestart%20%3D%20true%20%20%20%3B%20%u7A0B%u5E8F%u5F02%u5E38%u9000%u51FA%u540E%u81EA%u52A8%u91CD%u542F%0Astartretries%20%3D%203%20%20%20%20%20%3B%20%u542F%u52A8%u5931%u8D25%u81EA%u52A8%u91CD%u8BD5%u6B21%u6570%uFF0C%u9ED8%u8BA4%u662F%203%0A%23user%20%3D%20root%20%20%20%20%20%20%20%3B%20%u7528%u54EA%u4E2A%u7528%u6237%u542F%u52A8%0A%23redirect\_stderr%20%3D%20true%20%20%3B%20%u628A%20stderr%20%u91CD%u5B9A%u5411%u5230%20stdout%uFF0C%u9ED8%u8BA4%20false%0A%23stdout\_logfile\_maxbytes%20%3D%2020MB%20%20%3B%20stdout%20%u65E5%u5FD7%u6587%u4EF6%u5927%u5C0F%uFF0C%u9ED8%u8BA4%2050MB%0A%23stdout\_logfile\_backups%20%3D%2020%20%20%20%20%20%3B%20stdout%20%u65E5%u5FD7%u6587%u4EF6%u5907%u4EFD%u6570%0A%23stdout\_logfile%20%3D%20/var/log/supervisor/logstash.log%0A%60%60%60%0A%0A%u641E%u5B9A%uFF0C%u8FD9%u6837elk%u5C31%u5B8C%u6210%u54AF%u3002