重定向 < > >> <<

stdin 0 标准输入(读)

stdout 1 标准输出(写)

stderr 2 标准错误(写)

exec 修改文件描述符号

elasticsearch 单机安装

1 修改 /etc/hosts

2 安装 yum install -y java-1.8.0-openjdk

3 安装 yum install -y elasticsearch

修改配置文件 /etc/elasticsearch/elasticsearch.yml

network.host: 0.0.0.0

启动服务 systemctl start elasticsearch

浏览器访问验证 http://192.168.1.11:9200/

elasticsearch 集群安装

一共安装 5 台 ES 数据库节点

配置所有主机的 /etc/hosts

192.168.1.11 es1

192.168.1.12 es2

192.168.1.13 es3

192.168.1.14 es4

192.168.1.15 es5

在所有节点安装

yum install -y java-1.8.0-openjdk elasticsearch

修改配置文件

cluster.name: nsd1803

node.name: 本机主机名称

network.host: 0.0.0.0

discovery.zen.ping.unicast.hosts: ["es1", "es2", "es3"]

验证集群

http://192.168.1.11:9200/\_cluster/health?pretty

插件安装

/usr/share/elasticsearch/bin/plugin install ftp://192.168.1.254/public/bigdesk-master.zip

/usr/share/elasticsearch/bin/plugin install ftp://192.168.1.254/public/elasticsearch-head-master.zip

/usr/share/elasticsearch/bin/plugin install ftp://192.168.1.254/public/elasticsearch-kopf-master.zip

访问插件 head

http://192.168.1.11:9200/\_plugin/head

访问插件 kopf

http://192.168.1.11:9200/\_plugin/kopf

访问插件 bigdesk

http://192.168.1.11:9200/\_plugin/bigdesk

创建索引

curl -XPUT 'http://192.168.1.13:9200/tedu/' -d \

'{

"settings":{

"index":{

"number\_of\_shards": 5,

"number\_of\_replicas": 1

}

}

}'

增加数据 PUT

curl -XPUT "http://192.168.1.11:9200/nsd1803/teacher/2" -d \

'{

"title": "阶段2",

"name": {"first":"老逗比", "last":"丁丁"},

"age":52

}'

更改数据 POST

curl -XPOST "http://192.168.1.15:9200/nsd1803/teacher/3/\_update" -d \

'{

"doc": { "age":18 }

}'

查询与删除数据

curl -XGET "http://192.168.1.14:9200/nsd1803/teacher/1?pretty"

curl -XDELETE "http://192.168.1.14:9200/nsd1803/teacher/1?pretty"

kibana 配置 /opt/kibana/config/kibana.yml

server.port: 5601

server.host: "0.0.0.0"

elasticsearch.url: "http://es1:9200"

kibana.index: ".kibana"

kibana.defaultAppId: "discover"

elasticsearch.pingTimeout: 1500

elasticsearch.requestTimeout: 30000

elasticsearch.startupTimeout: 5000

数据批量导入

有 index, type, id 的导入

curl -XPOST http://192.168.1.13:9200/\_bulk --data-binary @shakespeare.json

无 index, type 有 id 的导入

curl -XPOST http://192.168.1.13:9200/oo/xx/\_bulk --data-binary @accounts.json

有 多个index,type 无 id 的导入

curl -XPOST http://192.168.1.13:9200/\_bulk --data-binary @logs.jsonl

数据批量查询

curl -XGET http://192.168.1.12:9200/\_mget?pretty -d '

{

docs:[

{"\_index": "oo",

"\_type": "xx",

"\_id": 99

},

{"\_index": "shakespeare",

"\_type": "act",

"\_id": 80730

},

{"\_index": "logstash-2015.05.20",

"\_type": "log",

"\_id": "AWTo2xXm16RGslV6jxJR"

}

]

}'

logstash 配置文件 logstash.conf

input{

stdin{ codec => "json" }

}

filter{

}

output{

stdout{ codec => "rubydebug" }

}

源码地址 https://github.com/logstash-plugins

文档地址 https://www.elastic.co/guide/en/logstash/current/index.html

file 模块

input {

... ...

file {

path => ["/tmp/a.log", "/tmp/b.log"]

sincedb\_path => "/var/lib/logstash/sincedb.log"

start\_position => "beginning"

type => "filelog"

}

}

tcp & udp 模块

input {

... ...

tcp {

mode => "server"

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp {

port => 9999

type => "udplog"

}

}

测试命令

echo "test udp log" >/dev/udp/192.168.1.20/9999

echo "test tcp log" >/dev/tcp/192.168.1.20/8888

syslog 模块

input {

... ...

syslog {

host => "0.0.0.0"

port => 514

type => "syslog"

}

}

客户机配置 @@(tcp) @(udp)

local0.info @@192.168.1.20:514

命令

logger -p local0.info -t "testlog" "hello world"

正则表达式分组匹配 (?<name>reg)

正则宏路径

/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns

filter{

grok{

match => ["message", "%{COMBINEDAPACHELOG}"]

}

}

output 输出到 Elasticsearch

增加类型判断，细化区分日志

output{

if [type] == "apachelog"{

elasticsearch {

hosts => ["192.168.1.15:9200", "192.168.1.11:9200"]

index => "apachelog"

flush\_size => 2000

idle\_flush\_time => 10

}}

}

使用 filebeat 收集日志，发送到 logstash

logstash beats 配置

input{

... ...

beats{

port => 5044

}

}

客户端配置

filebeat:

prospectors:

-

paths:

- /var/log/httpd/access\_log

input\_type: log

document\_type: apachelog

registry\_file: /var/lib/filebeat/registry

output:

logstash:

hosts: ["192.168.1.20:5044"]

shipper:

logging:

files:

rotateeverybytes: 10485760 # = 10MB