filebeat1192.168.10.11

filebeat2192.168.10.12 —> logstash192.168.10.20 --> elasticse192.168.10.30 --> kibana192.168.10.40

filebeat3192.168.10.13

说明：

ly-tomcat\_web项目在主机10.11上做双机负载

tags: "ly-tomcat-web"

 10.11 - /data/ly-tomcat\_web1/logs/catalina.out

10.11 - /data/ly-tomcat\_web2/logs/catalina.out

ly-tomcat\_admin项目在主机10.11 上单机

tags: "ly-tomcat-admin"

 10.11 - /data/ly-tomcat\_admin/logs/catalina.out

spring\_could 项目在主机10.12和10.12上做双机负载

tags: "spring\_could-gate"

10.13 - /data/spring\_could/gate.log

tags: "spring\_could-auth"

 10.12 - /data/spring\_could/auth.log

 10.13 - /data/spring\_could/auth.log

tags: "spring\_could-order"

 10.12 - /data/spring\_could/order.log

 10.13 - /data/spring\_could/order.log

1.filebeat

1.1 filebeat1(192.168.10.11)

*# vim /etc/filebeat/filebeat.yml*

filebeat.prospectors:

- input\_type: log

 paths:

 - /data/ly-tomcat\_web1/logs/catalina.out

 - /data/ly-tomcat\_web2/logs/catalina.out

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: "ly-tomcat-web"

- input\_type: log

 paths:

 - /data/ly-tomcat\_admin/logs/catalina.out

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: "ly-tomcat-admin"

setup.kibana:

 host: "192.168.10.40:5601"

output.logstash:

 hosts: ["192.168.10.20:5044"]

1.2 filebeat2(192.168.10.12)

*# vim /etc/filebeat/filebeat.yml*

filebeat.prospectors:

- input\_type: log

 paths:

 - /data/spring\_could/auth.log

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: "spring\_could-auth"

- input\_type: log

 paths:

 - /data/spring\_could/order.log

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: " spring\_could-order"

setup.kibana:

 host: "192.168.10.40:5601"

output.logstash:

 hosts: ["192.168.10.20:5044"]

1.3 filebeat3(192.168.10.13)

*# vim /etc/filebeat/filebeat.yml*

filebeat.prospectors:

- input\_type: log

 paths:

 - /data/spring\_could/gate.log

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: " spring\_could-gate"

- input\_type: log

 paths:

 - /data/spring\_could/auth.log

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: "spring\_could-auth"

- input\_type: log

 paths:

 - /data/spring\_could/order.log

 exclude\_lines: ['TRACE']

 encoding: "utf-8"

 tags: "spring\_could-order"

setup.kibana:

 host: "192.168.10.40:5601"

output.logstash:

 hosts: ["192.168.10.20:5044"]

2.logstash

2.1 ly项目

*# vim /etc/logstash/conf.d/ly.conf*

input {

 beats {

 port => "5044"

 }

}

output {

 if "ly-tomcat-web" in [tags] {

 elasticsearch {

 hosts => ["192.168.10.30:9200"]

 index => "ly-tomcat-web-%{+YYYY.MM}"

 manage\_template => true

 }

 }

 else if "ly-tomcat-admin" in [tags] {

 elasticsearch {

 hosts => ["192.168.10.30:9200"]

 index => "lyw-tomcat-admin-%{+YYYY.MM}"

 manage\_template => true

 }

 }

}

2.2 spring\_could项目

*# vim /etc/logstash/conf.d/spring\_could.conf*

input {

 beats {

 port => "5044"

 }

}

output {

 if "spring\_could-gate" in [tags] {

 elasticsearch {

 hosts => ["192.168.10.30:9200"]

 index => "spring\_could-gate-%{+YYYY.MM}"

 manage\_template => true

 }

 }

 else if "spring\_could-auth" in [tags] {

 elasticsearch {

 hosts => ["192.168.10.30:9200"]

 index => "spring\_could-auth-%{+YYYY.MM}"

 manage\_template => true

 }

 }

 else if "spring\_could-order" in [tags] {

 elasticsearch {

 hosts => ["192.168.10.30:9200"]

 index => "spring\_could-orde-%{+YYYY.MM}"

 manage\_template => true

 }

 }

}

3.elasticsearch(192.168.10.30)

*# vim /etc/elasticsearch/elasticsearch.yml*

cluster.name: ych-ELK

node.name: ELK-01

path.data: /data/elasticsearch

path.logs: /data/logs/elasticsearch

network.host: 0.0.0.0

http.port: 9200

http.cors.enabled: true

http.cors.allow-origin: "\*"

4.kibana(192.168.10.40)

4.2 kibana

*# vim /etc/kibana/kibana.yml*

server.port: 5601

server.host: "192.168.10.40"

elasticsearch.url: <http://192.168.10.30:9200>

4.2 kibana添加索引

*http://192.168.10.40*

lyw-tomcat-web\*

lyw-tomcat-admin\*

spring\_could-gate\*

spring\_could-auth\*

spring\_could-orde\*