#ELK5.4.3安装配置说明文档

Credited

- by 李杨
- update 2017/7/20

#单机部署

##elasticsearch

- Failed to created node environment · Issue #21 · elastic/elasticsearch-docker

Elasticsearch 5.4.3 镜像的用户为(uid: 1000, gid: 1000)，必须先将data授权给Elasticsearch的用户。

- Graham Dumpleton: Don't run as root inside of Docker containers. 介绍了Elasticsearch为什么不用root用户

```
#ES节点
curl 'localhost:9200/_cat/nodes?v'
#创建数据和配置文件的目录
mkdir -p /data/elasticsearch/data/nodes
mkdir -p /data/elasticsearch/config
#修改文件夹权限
chown -R 1000.1000 /data/elasticsearch
#索引
curl localhost:9201/_cat/indices?v
#数据
curl localhost:9201/_search
```

```
docker run -dti --restart=always --name elasticsearch \
  -e ES_JAVA_OPTS="-Xms1g -Xmx1g -Duser.timezone=GMT+08" \
  -v /data/elasticsearch/data:/usr/share/elasticsearch/data \
  -v
/data/elasticsearch/config/elasticsearch.yml:/usr/share/elasticsearch/config/e
lasticsearch.yml \
  -v /etc/localtime:/etc/localtime \
```

```
  -p 9200:9200 \
  -p 9300:9300 \
  docker.elastic.co/elasticsearch/elasticsearch:5.4.3
```

elasticsearch.yml

```
---
## Default Elasticsearch configuration from elasticsearch-docker.
## from https://github.com/elastic/elasticsearch-
docker/blob/master/build/elasticsearch/elasticsearch.yml
#
cluster.name: "docker-cluster"
network.host: 0.0.0.0

# minimum_master_nodes need to be explicitly set when bound on a public IP
# set to 1 to allow single node clusters
# Details: https://github.com/elastic/elasticsearch/pull/17288
discovery.zen.minimum_master_nodes: 1

## Use single node discovery in order to disable production mode and avoid
bootstrap checks
## see
https://www.elastic.co/guide/en/elasticsearch/reference/current/bootstrap-
checks.html
#
discovery.type: single-node

## Disable X-Pack
## see https://www.elastic.co/guide/en/x-pack/current/xpack-settings.html
##     https://www.elastic.co/guide/en/x-pack/current/installing-
xpack.html#xpack-enabling
#
xpack.security.enabled: false
xpack.monitoring.enabled: false
xpack.ml.enabled: false
xpack.graph.enabled: false
xpack.watcher.enabled: false
```

##logstash

```
docker run -dti --restart=always --name logstash \
  -e LS_JAVA_OPTS="-Xmx256m -Xms256m" \
  -v ./logstash/config/logstash.yml:/usr/share/logstash/config/logstash.yml \
  -v ./logstash/pipeline:/usr/share/logstash/pipeline \
  -p 5000:5000 \
  docker.elastic.co/logstash/logstash:5.4.3
```

logstash/config/logstash.yml

```
---
## Default Logstash configuration from logstash-docker.
## from https://github.com/elastic/logstash-
docker/blob/master/build/logstash/config/logstash.yml
#
http.host: "0.0.0.0"
path.config: /usr/share/logstash/pipeline

## Disable X-Pack
## see https://www.elastic.co/guide/en/x-pack/current/xpack-settings.html
##     https://www.elastic.co/guide/en/x-pack/current/installing-
xpack.html#xpack-enabling
#
xpack.monitoring.enabled: false
```

logstash/pipeline/logstash.conf

```
input {
        beats {
                port => "5000"
        }
}

filter {
        ruby {
                code => 'msgs = event.get("message").split("§|§")
            event.set("time_local", msgs[0])
            event.set("hostname", msgs[1])
            event.set("remote_addr", msgs[2])
            event.set("remote_port", msgs[3])
            event.set("remote_user", msgs[4])
            event.set("scheme", msgs[5])
            event.set("request_method", msgs[6])
            event.set("uri", msgs[7])
            event.set("request_uri", msgs[8])
            event.set("request_filename", msgs[9])
            event.set("args", msgs[10])
            event.set("http_user_agent", msgs[11])
            event.set("http_referer", msgs[12])
            event.set("http_x_forwarded_for", msgs[13])
            event.set("content_length", msgs[14])
            event.set("content_type", msgs[15])
            event.set("body_bytes_sent", msgs[16])
            event.set("request_body", msgs[17])
            event.set("status", msgs[18])
            event.set("server_addr", msgs[19])
            event.set("server_name", msgs[20])
```

```
            event.set("server_port", msgs[21])
            event.set("server_protocol", msgs[22])
            event.set("request_time", msgs[23])
            event.set("upstream_response_time", msgs[24])
            event.set("proxy_add_x_forwarded_for", msgs[25])
            event.set("upstream_addr", msgs[26])
            event.set("request_type", msgs[7].split(".").last)
        '
        }
        mutate {
                convert => [
                        "body_bytes_sent", "integer",
                        "content_length", "integer",
                        "server_port", "integer",
                        "remote_port", "integer",
                        "status", "integer",
                        "upstream_response_time", "float",
                        "request_time", "float"
                ]
        }
}
output {
        elasticsearch {
                hosts => "elasticsearch:9200"
        }
        stdout {
                codec => rubydebug
        }
}
```

##filebeat

```
output:
  logstash:
    enabled: true
    hosts:
      - 192.168.31.215:5000

filebeat:
  prospectors:
    -
      paths:
        - "/var/log/nginx/*.log"
      document_type: nginx-access
```

##nginx

/etc/nginx/nginx.conf

```
user  root;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;

events {
    worker_connections  1024;
}


http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  $time_local§|§$hostname§|§$remote_addr§|§$remote_port§|§
$remote_user§|§'
        '$scheme§|§$request_method§|§$uri§|§$request_uri§|§$request_filename§|
§'
        '$args§|§[$http_user_agent]§|§$http_referer§|§$http_x_forwarded_for§|
§'
        '$content_length§|§$content_type§|§'
        '$body_bytes_sent§|§$request_body§|§$status§|§'
        '$server_addr§|§$server_name§|§$server_port§|§$server_protocol§|§'
        '$request_time§|§$upstream_response_time§|§
$proxy_add_x_forwarded_for§|§$upstream_addr';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

    include /etc/nginx/conf.d/*.conf;
}
```

#集群部署

##elasticsearch

集群需要注意时区一致。

```
#时区
cp -f /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
#ES节点
curl 'localhost:9200/_cat/nodes?v'
```

```
#创建数据和配置文件的目录
mkdir -p /data/elasticsearch1/data
mkdir -p /data/elasticsearch1/config
mkdir -p /data/elasticsearch2/data
mkdir -p /data/elasticsearch2/config
mkdir -p /data/elasticsearch3/data
mkdir -p /data/elasticsearch3/config
#修改文件夹权限
chown -R 1000.1000 /data/elasticsearch1
chown -R 1000.1000 /data/elasticsearch2
chown -R 1000.1000 /data/elasticsearch3
#索引
curl localhost:9201/_cat/indices?v
#数据
curl localhost:9201/_search
```

```
#elasticsearch 版本 5.4.3 集群部署
docker run -dti --restart=always --name elk-1 \
  -e ES_JAVA_OPTS="-Xms1g -Xmx1g -Duser.timezone=GMT+08" \
  -v /data/elasticsearch1/data:/usr/share/elasticsearch/data \
  -v
/data/elasticsearch1/config/elasticsearch.yml:/usr/share/elasticsearch/config/
elasticsearch.yml \
  -v /etc/localtime:/etc/localtime \
  -p 9201:9200 \
  -p 9301:9300 \
  docker.elastic.co/elasticsearch/elasticsearch:5.4.3
docker run -dti --restart=always --name elk-2 \
  -e ES_JAVA_OPTS="-Xms1g -Xmx1g -Duser.timezone=GMT+08" \
  -v /data/elasticsearch2/data:/usr/share/elasticsearch/data \
  -v
/data/elasticsearch2/config/elasticsearch.yml:/usr/share/elasticsearch/config/
elasticsearch.yml \
  -v /etc/localtime:/etc/localtime \
  -p 9202:9200 \
  -p 9302:9300 \
  docker.elastic.co/elasticsearch/elasticsearch:5.4.3
docker run -dti --restart=always --name elk-3 \
  -e ES_JAVA_OPTS="-Xms1g -Xmx1g -Duser.timezone=GMT+08" \
  -v /data/elasticsearch3/data:/usr/share/elasticsearch/data \
  -v
/data/elasticsearch3/config/elasticsearch.yml:/usr/share/elasticsearch/config/
elasticsearch.yml \
  -v /etc/localtime:/etc/localtime \
  -p 9203:9200 \
  -p 9303:9300 \
  docker.elastic.co/elasticsearch/elasticsearch:5.4.3
```

elasticsearch.yml

```
---
## Default Elasticsearch configuration from elasticsearch-docker.
## from https://github.com/elastic/elasticsearch-
docker/blob/master/build/elasticsearch/elasticsearch.yml
#
cluster.name: "docker-cluster"
network.host: 0.0.0.0

# minimum_master_nodes need to be explicitly set when bound on a public IP
# set to 1 to allow single node clusters
# Details: https://github.com/elastic/elasticsearch/pull/17288
discovery.zen.minimum_master_nodes: 1
discovery.zen.ping.unicast.hosts:
["192.168.31.215:9301","192.168.31.215:9302"]

## Disable X-Pack
## see https://www.elastic.co/guide/en/x-pack/current/xpack-settings.html
##     https://www.elastic.co/guide/en/x-pack/current/installing-
xpack.html#xpack-enabling
#
xpack.security.enabled: false
xpack.monitoring.enabled: false
xpack.ml.enabled: false
xpack.graph.enabled: false
xpack.watcher.enabled: false
```