监控程序部署安装手册

# Fluentd安装

## 安装前配置

1. 查询并修改文件描述符

$ulimit –n

1024

如果值小于65536，可以使用如下命令进行配置

$vi /etc/security/limit.conf

#增加配置信息

root soft nofile 65536

root hard nofile 65536

\* soft nofile 65536

\* hard nofile 65536

1. 优化网络设置

$vi /etc/sysctl.conf

#增加配置信息

net.ipv4.tcp\_tw\_recycle = 1

net.ipv4.tcp\_tw\_reuse = 1

net.ipv4.ip\_local\_port\_range = 10240 65535

## 安装fluentd

1. 执行安装命令（网络安装，使用root权限）

#redhat or centos

$curl -L https://toolbelt.treasuredata.com/sh/install-redhat-td-agent2.sh | sh

其它系统可以参考官网安装文档。

**本地安装**

#centos 6

$rpm –i td-agent-2.2.1-0.el6.x86\_64.rpm

#centos 7

$rpm –i td-agent-2.2.1-0.el7.x86\_64.rpm

1. 运行服务，可以执行如下命令（启动、停止、重启、查询状态）：

$/etc/init.d/td-agent start

$/etc/init.d/td-agent stop

$/etc/init.d/td-agent restart

$/etc/init.d/td-agent status

或者

$service td-agent start

$service td-agent stop

$service td-agent restart

$service td-agent status

## 设置自启动

$chkconfig td-agent on

## 配置文件

Fluentd的配置文件默认存放在：/etc/td-agent/ta-agent.conf路径下。

安装目录存放在：/opt/td-agent/目录下

嵌入的ruby放在：/opt/td-agent/embedded/bin目录下

日志文件默认存放在：/var/log/td-agent/目录下

### 采集端配置

## input

<source>

type tail

format /^(?<request\_time>[^|]\*)\|(?<app\_name>[^|]\*)\|(?<log\_type>[^|]\*)\|(?<client\_ip>[^:]\*):(?<client\_port>[^|]\*)\|(?<server\_ip>[^:]\*):(?<server\_port>[^|]\*)\|(?<elapsed\_time>[^|]\*)\|(?<communication\_type>[^|]\*)\|(?<req\_length>[^|]\*)\|(?<resp\_length>[^|]\*)\|(?<method>[^|]\*)\|(?<url>[^|]\*)\|(?<status\_code>[^|]\*)\|(?<query\_entity>[^|]\*)\|(?<call\_method>[^|]\*)\|(?<business\_code>[^|]\*)\|(?<return content>[^|]\*)$/

path /opt/uiac/uiacserver/logs/quality\_access.log

pos\_file /var/log/td-agent/access/quality\_access.log.pos

tag quality\_access

</source>

## output

<match quality\_access>

type forward

send\_timeout 30s

recover\_wait 10s

heartbeat\_interval 10s

heartbeat\_type udp

buffer\_type memory

flush\_interval 10s

num\_threads 1

<server>

name master\_server

host 192.168.6.60

port 24235

</server>

<server>

name bak\_server

host 192.168.6.61

port 24235

</server>

<secondary>

type file

path /var/log/td-agent/access/send-failed

</secondary>

</match>

注：

1. 黄色标记的文本是可修改，其中:path xxxxxx，后面的内容为实际需要采集的应用日志路径
2. Server节点是指采集服务器的配置，有多个则配置多个

### 服务端配置

1. 服务端需要安装fluentd插件，执行如下步骤：

*#更改gem 源为国内淘宝源*

*/opt/td-agent/embedded/bin/gem sources –a* [*https://ruby.taobao.org/*](https://ruby.taobao.org/) *–r* [*https://rubygems.org/*](https://rubygems.org/)

*#安装插件*

*/opt/td-agent/embedded/bin/gem install fluent-plugin-elasticsearch*

## input

<source>

type forward

port 24235

</source>

# Store Data in Elasticsearch

<match quality\_access>

  type copy

  <store>

    type elasticsearch

    host localhost

    port 9200

    include\_tag\_key true

    tag\_key app\_name

    logstash\_format true

logstash\_dateformat %Y%m%d

logstash\_prefix quality\_day

buffer\_chunk\_limit 32m

flush\_interval 5s

  </store>

</match>

注：黄色文本需要修改成ES的服务器地址及端口，多个服务器之间用逗号（，）分隔

# ElasticSearch安装

## 环境配置

ElasticSearch运行需要java7及以上的版本支持，请确保系统中已安装对应版本的软件，建议安装的版本为Oracle Java 1.7+环境。

在官网下载elasticsearch最新的2.X版本，解压到运行目录（/opt/deploy）。

## 参数配置

找到解压目录下的conf目录，如：

$cd elasticsearch-2.1.0/config

$vi elasticsearch.yml

注：elasticsearch-2.1.0可修改为实际的程序目录

在elasticsearch.yml文件中，常见配置项如下

# 集群名称，此处统一为quality\_log

cluster.name: quality\_log

# 节点名称，此处约定格式为：node-{ip}，{ip}为后两段值，点号替换为下划线

node.name: node-30\_65

# 索引数据存放路径，可配置多个目录，用逗号分隔

path.data: /u01/es/data

# 日志数据存放路径

path.logs: /u01/es/logs

# 当前实例监听监听服务IP

network.host: 192.168.30.65

# 监听服务端口

http.port: 9200

# 在N个节点启动后才允许恢复处理

gateway.recover\_after\_nodes: 2

# 设置集群中期望的节点数目，一般为集群机器总数

gateway.expected\_nodes: 3

# 设置初始化恢复过程的超时时间，即超达到恢复处理的节点数后，等待指定时间后开始恢复处理，如果节点数目达到期望节点，则直接开始恢复

gateway.recover\_after\_time: 3m

# 探查时间，默认为3秒，可以调整大一些以防止网络情况不好的时候

discovery.zen.ping.timeout: 3s

# 是否启用多播，此处设置为禁用

discovery.zen.ping.multicast.enable: false

# 集群中主节点的初始列表

discovery.zen.ping.unicast.hosts: ["192.168.30.65", "192.168.30.66", "192.168.30.67"]

# 集群中有Master资格的最小节点数

discovery.zen.minimum\_master\_nodes: 2

**启动参数内存配置：**

找到安装目录bin目录下的elasticsearch.in.sh，此文件可以设置JAVA的一些环境，此项目中只需要根据机器内存情况设置ES\_MIN\_MEM和ES\_MAX\_MEM参数，建议最小值设置为2g，最大内存根据服务器机器状态而定。

## 插件安装

可以安装一个集群管理的插件，方便查询集群状态

./elasticsearch/bin/plugin install lmenezes/elasticsearch-kopf/{branch|version}

访问地址如下：

http://localhost:9200/\_plugin/kopf

## 运行

执行:./elasticsearch –d开始

## 初始化索引模板

索引元数据模板存放在:logmapping\_template.json文件中。可以执行如下命令创建模板

curl –XPUT <http://localhost:9200/_template/quality_template> -d @logmapping\_template.json

# Kibana安装

## 环境配置

Kibana运行需要java7及以上的版本支持，请确保系统中已安装对应版本的软件，建议安装的版本为Oracle Java 1.7+环境。

在官网下载elasticsearch最新的2.X版本，解压到运行目录（/opt/deploy）。

## 参数配置

找到解压目录下的config目录，修改kibana.yml文件，将下面的参数修改为实际的ES服务器地址：

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

## 启动程序

nohup ./kibana > /path/log/kibana.log 2>&1 &

上面指令中，红色部份可以修改为实际存储日志的路径