Crontab及logstash

# 1.Crontab

Crontab命令，用户设置周期性被执行的指令。该命令从标准输入设备读取指定，并将其存放在crontab文件中，以供之后的读取和执行。通常crontab储存的指令被守护进程激活，crond常常在后台运行，每一分钟检查是否有预定的作业需要执行，这类作业一般称为cron jobs。

## 1.1 Crontab文件

该文件包含送交cron守护进程的一系列作业和指令。每个用户可以拥有自己的crontab文件；同时，操作系统保存一个针对整个系统的crontab文件，该文件通常存放于/etc/或者/etc之下的子目录中，而这个文件由系统管理员来修改。/etc/crontab的格式如下：

SHELL=/bin/bash

PATH=/sbin:/bin:/usr/sbin:/usr/bin

MAILTO=root

HOME=/

# For details see man 4 crontabs

# Example of job definition:

# .---------------- minute (0 - 59)

# | .------------- hour (0 - 23)

# | | .---------- day of month (1 - 31)

# | | | .------- month (1 - 12) OR jan,feb,mar,apr ...

# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat

# | | | | |

# \* \* \* \* \* user-name command to be executed

前四行，用来设置crontab任务运行环境的变量。SHELL变量的值告诉系统要使用哪个Shell环境。

## 1.2 crond服务启停

Crontab周期执行指令，通过后台crond来控制，crond的命令

Usage: /etc/init.d/crond {start|stop|status|restart|condrestart|try-restart|reload|force-reload}

启动命令如下：

$service crond start

停止命令如下：

$service crond stop

## 1.3 Crontab使用案例

用户Strom定义crontab定时任务，每分钟在用户目录下的log.txt中写入当前日期时间。

登录用户storm:

$su - storm

1）第一次使用crontab，显示以下信息：

[storm@bdi32 ~]$ crontab -e

no crontab for storm - using an empty one

根据提示，输入

\*/1 \* \* \* \* date >> /home/storm/log.txt

保存退出后，提示：

crontab: installing new crontab

2）登录root，重启crond服务

$service crond restart

在目录/var/spool/cron下，可以看到storm文件，

3）切换到storm

$ crontab -l

\*/1 \* \* \* \* date >> /home/storm/log.txt

4）查看运行结果

$tail -f log.txt

输出结果如下：

[storm@bdi33 ~]$ tail -f log.txt

Fri Aug 21 10:59:01 CST 2015

## 1.4 用户删除定时服务

在该用户下执行：

$crontab -r

# 2.logstash

## 2.1安装和使用

Logstash是开源的日志管理工具，可以对日志进行收集、分析，并将其存储供以后使用（如，搜索），另外logstash带有一个web界面，搜索和展示所有日志。Logstash可以看做是一个数据管道，可以从不同的系统来源收集日志或者其他事件数据，并将数据传送到统一的中央分析系统中。

1）下载logstash

wget http://download.elastic.co/logstash/logstash/logstash-1.5.0.zip

2)解压并修改配置文件

logstash.conf中的配置项，包括：

input { #输入配置

stdin { }

}

output { #输出配置

stdout {

codec => rubydebug

}

}

3）启动命令

bin/logstash -f logstash.conf

4）查看logstash的输出内容

[storm@bdi31 logstash-1.5.0]$ bin/logstash -f config/logstash.conf

Logstash startup completed

#hello

2015-08-28T02:31:53.575Z bdi31.cmss.com hello

启动后，控制台输入hello，后输出下面的一行内容

5）配置crontab日志文件作为输入

input

{

file{

path => "/home/storm/data/test.log"

start\_position => beginning

}

}

当在日志输入新数据时，

[storm@bdi31 data]$ echo hello logstash >> test.log

控制台输出如下：

2015-08-28T02:46:28.362Z bdi31.cmss.com hello logstash

## 2.2 Logstash kafka

Logstash的写入日志，写到kafka中后，传到storm进行处理，配置如下：

output

{

kafka{

broker\_list => "bdi31.cmss.com:9092"

topic\_id => "stormtest"

codec => plain {

format => "%{message}"

}

}

}

## 2.3 Elasticsearch及Kibana

Elasticsearch:实时分布式搜索及分析工具，基于Apache Lucene基础上的搜索引擎

Kibana: 基于浏览器页面的Elasticsearch前端展示工具

# 参考文献

http://www.111cn.net/sys/linux/64414.htm

http://www.2cto.com/os/201411/352015.html

http://www.ttlsa.com/log-system/installing-logstash-on-rhel-and-centos/

https://github.com/bigbo/logstash-best-practice-cn

https://github.com/joekiller/logstash-kafka

Elasticsearch: http://www.learnes.net/