ELK是一套解决方案

包括：Easticsearch、Logstash、Kibana三个部分

环境：

192.168.4.20—elk01

192.168.4.21—es01

192.168.4.22—es02

192.168.4.23—es03

192.168.4.24—es04

关闭防火墙、SELinux

##配置域名解析

[root@elk01 ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.4.20 elk

192.168.4.21 es01

192.168.4.22 es02

192.168.4.23 es03

192.168.4.24 es04

#五台同步

##安装jdk

[root@elk01 ~]# yum -y install java-1.8.0-openjdk java-1.8.0-openjdk-devel

已加载插件：langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

正在解决依赖关系

--> 正在检查事务

---> 软件包 java-1.8.0-openjdk.x86\_64.1.1.8.0.102-4.b14.el7 将被 安装

--> 正在处理依赖关系 java-1.8.0-openjdk-headless = 1:1.8.0.102-4.b14.el7，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 fontconfig(x86-64)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libjava.so(SUNWprivate\_1.1)(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libjvm.so(SUNWprivate\_1.1)(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 xorg-x11-fonts-Type1，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libXcomposite.so.1()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libXext.so.6()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libXi.so.6()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libXrender.so.1()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libXtst.so.6()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libawt.so()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libgif.so.4()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libjava.so()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 libjvm.so()(64bit)，它被软件包 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 需要

---> 软件包 java-1.8.0-openjdk-devel.x86\_64.1.1.8.0.102-4.b14.el7 将被 安装

--> 正在检查事务

---> 软件包 fontconfig.x86\_64.0.2.10.95-10.el7 将被 安装

--> 正在处理依赖关系 fontpackages-filesystem，它被软件包 fontconfig-2.10.95-10.el7.x86\_64 需要

---> 软件包 giflib.x86\_64.0.4.1.6-9.el7 将被 安装

--> 正在处理依赖关系 libICE.so.6()(64bit)，它被软件包 giflib-4.1.6-9.el7.x86\_64 需要

--> 正在处理依赖关系 libSM.so.6()(64bit)，它被软件包 giflib-4.1.6-9.el7.x86\_64 需要

---> 软件包 java-1.8.0-openjdk-headless.x86\_64.1.1.8.0.102-4.b14.el7 将被 安装

--> 正在处理依赖关系 copy-jdk-configs >= 1.1-3，它被软件包 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 tzdata-java >= 2015d，它被软件包 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 jpackage-utils，它被软件包 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_64 需要

--> 正在处理依赖关系 lksctp-tools(x86-64)，它被软件包 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_64 需要

---> 软件包 libXcomposite.x86\_64.0.0.4.4-4.1.el7 将被 安装

---> 软件包 libXext.x86\_64.0.1.3.3-3.el7 将被 安装

---> 软件包 libXi.x86\_64.0.1.7.4-2.el7 将被 安装

---> 软件包 libXrender.x86\_64.0.0.9.8-2.1.el7 将被 安装

---> 软件包 libXtst.x86\_64.0.1.2.2-2.1.el7 将被 安装

---> 软件包 xorg-x11-fonts-Type1.noarch.0.7.5-9.el7 将被 安装

--> 正在处理依赖关系 mkfontdir，它被软件包 xorg-x11-fonts-Type1-7.5-9.el7.noarch 需要

--> 正在处理依赖关系 mkfontdir，它被软件包 xorg-x11-fonts-Type1-7.5-9.el7.noarch 需要

--> 正在处理依赖关系 ttmkfdir，它被软件包 xorg-x11-fonts-Type1-7.5-9.el7.noarch 需要

--> 正在处理依赖关系 ttmkfdir，它被软件包 xorg-x11-fonts-Type1-7.5-9.el7.noarch 需要

--> 正在检查事务

---> 软件包 copy-jdk-configs.noarch.0.1.2-1.el7 将被 安装

---> 软件包 fontpackages-filesystem.noarch.0.1.44-8.el7 将被 安装

---> 软件包 javapackages-tools.noarch.0.3.4.1-11.el7 将被 安装

--> 正在处理依赖关系 python-javapackages = 3.4.1-11.el7，它被软件包 javapackages-tools-3.4.1-11.el7.noarch 需要

---> 软件包 libICE.x86\_64.0.1.0.9-2.el7 将被 安装

---> 软件包 libSM.x86\_64.0.1.2.2-2.el7 将被 安装

---> 软件包 lksctp-tools.x86\_64.0.1.0.17-2.el7 将被 安装

---> 软件包 ttmkfdir.x86\_64.0.3.0.9-42.el7 将被 安装

---> 软件包 tzdata-java.noarch.0.2016g-2.el7 将被 安装

---> 软件包 xorg-x11-font-utils.x86\_64.1.7.5-20.el7 将被 安装

--> 正在处理依赖关系 libXfont.so.1()(64bit)，它被软件包 1:xorg-x11-font-utils-7.5-20.el7.x86\_64 需要

--> 正在处理依赖关系 libfontenc.so.1()(64bit)，它被软件包 1:xorg-x11-font-utils-7.5-20.el7.x86\_64 需要

--> 正在检查事务

---> 软件包 libXfont.x86\_64.0.1.5.1-2.el7 将被 安装

---> 软件包 libfontenc.x86\_64.0.1.1.2-3.el7 将被 安装

---> 软件包 python-javapackages.noarch.0.3.4.1-11.el7 将被 安装

--> 解决依赖关系完成

依赖关系解决

================================================================================

Package 架构 版本 源 大小

================================================================================

正在安装:

java-1.8.0-openjdk x86\_64 1:1.8.0.102-4.b14.el7 development 230 k

java-1.8.0-openjdk-devel x86\_64 1:1.8.0.102-4.b14.el7 development 9.7 M

为依赖而安装:

copy-jdk-configs noarch 1.2-1.el7 development 14 k

fontconfig x86\_64 2.10.95-10.el7 development 229 k

fontpackages-filesystem noarch 1.44-8.el7 development 9.9 k

giflib x86\_64 4.1.6-9.el7 development 40 k

java-1.8.0-openjdk-headless x86\_64 1:1.8.0.102-4.b14.el7 development 31 M

javapackages-tools noarch 3.4.1-11.el7 development 73 k

libICE x86\_64 1.0.9-2.el7 development 65 k

libSM x86\_64 1.2.2-2.el7 development 39 k

libXcomposite x86\_64 0.4.4-4.1.el7 development 22 k

libXext x86\_64 1.3.3-3.el7 development 39 k

libXfont x86\_64 1.5.1-2.el7 development 150 k

libXi x86\_64 1.7.4-2.el7 development 40 k

libXrender x86\_64 0.9.8-2.1.el7 development 26 k

libXtst x86\_64 1.2.2-2.1.el7 development 20 k

libfontenc x86\_64 1.1.2-3.el7 development 30 k

lksctp-tools x86\_64 1.0.17-2.el7 development 88 k

python-javapackages noarch 3.4.1-11.el7 development 31 k

ttmkfdir x86\_64 3.0.9-42.el7 development 48 k

tzdata-java noarch 2016g-2.el7 development 180 k

xorg-x11-font-utils x86\_64 1:7.5-20.el7 development 87 k

xorg-x11-fonts-Type1 noarch 7.5-9.el7 development 521 k

事务概要

================================================================================

安装 2 软件包 (+21 依赖软件包)

总下载量：43 M

安装大小：146 M

Downloading packages:

(1/23): copy-jdk-configs-1.2-1.el7.noarch.rpm | 14 kB 00:00

(2/23): fontpackages-filesystem-1.44-8.el7.noarch.rpm | 9.9 kB 00:00

(3/23): fontconfig-2.10.95-10.el7.x86\_64.rpm | 229 kB 00:00

(4/23): giflib-4.1.6-9.el7.x86\_64.rpm | 40 kB 00:00

(5/23): java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64.rpm | 230 kB 00:00

(6/23): java-1.8.0-openjdk-devel-1.8.0.102-4.b14.el7.x86\_6 | 9.7 MB 00:00

(7/23): javapackages-tools-3.4.1-11.el7.noarch.rpm | 73 kB 00:00

(8/23): libICE-1.0.9-2.el7.x86\_64.rpm | 65 kB 00:00

(9/23): libSM-1.2.2-2.el7.x86\_64.rpm | 39 kB 00:00

(10/23): libXcomposite-0.4.4-4.1.el7.x86\_64.rpm | 22 kB 00:00

(11/23): java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x | 31 MB 00:00

(12/23): libXext-1.3.3-3.el7.x86\_64.rpm | 39 kB 00:00

(13/23): libXi-1.7.4-2.el7.x86\_64.rpm | 40 kB 00:00

(14/23): libXfont-1.5.1-2.el7.x86\_64.rpm | 150 kB 00:00

(15/23): libXrender-0.9.8-2.1.el7.x86\_64.rpm | 26 kB 00:00

(16/23): libXtst-1.2.2-2.1.el7.x86\_64.rpm | 20 kB 00:00

(17/23): libfontenc-1.1.2-3.el7.x86\_64.rpm | 30 kB 00:00

(18/23): lksctp-tools-1.0.17-2.el7.x86\_64.rpm | 88 kB 00:00

(19/23): python-javapackages-3.4.1-11.el7.noarch.rpm | 31 kB 00:00

(20/23): tzdata-java-2016g-2.el7.noarch.rpm | 180 kB 00:00

(21/23): ttmkfdir-3.0.9-42.el7.x86\_64.rpm | 48 kB 00:00

(22/23): xorg-x11-font-utils-7.5-20.el7.x86\_64.rpm | 87 kB 00:00

(23/23): xorg-x11-fonts-Type1-7.5-9.el7.noarch.rpm | 521 kB 00:00

--------------------------------------------------------------------------------

总计 32 MB/s | 43 MB 00:01

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

正在安装 : libXext-1.3.3-3.el7.x86\_64 1/23

正在安装 : libXi-1.7.4-2.el7.x86\_64 2/23

正在安装 : libfontenc-1.1.2-3.el7.x86\_64 3/23

正在安装 : libICE-1.0.9-2.el7.x86\_64 4/23

正在安装 : libSM-1.2.2-2.el7.x86\_64 5/23

正在安装 : giflib-4.1.6-9.el7.x86\_64 6/23

正在安装 : libXfont-1.5.1-2.el7.x86\_64 7/23

正在安装 : 1:xorg-x11-font-utils-7.5-20.el7.x86\_64 8/23

正在安装 : libXtst-1.2.2-2.1.el7.x86\_64 9/23

正在安装 : tzdata-java-2016g-2.el7.noarch 10/23

正在安装 : copy-jdk-configs-1.2-1.el7.noarch 11/23

正在安装 : lksctp-tools-1.0.17-2.el7.x86\_64 12/23

正在安装 : libXrender-0.9.8-2.1.el7.x86\_64 13/23

正在安装 : libXcomposite-0.4.4-4.1.el7.x86\_64 14/23

正在安装 : python-javapackages-3.4.1-11.el7.noarch 15/23

正在安装 : javapackages-tools-3.4.1-11.el7.noarch 16/23

正在安装 : ttmkfdir-3.0.9-42.el7.x86\_64 17/23

正在安装 : fontpackages-filesystem-1.44-8.el7.noarch 18/23

正在安装 : fontconfig-2.10.95-10.el7.x86\_64 19/23

正在安装 : xorg-x11-fonts-Type1-7.5-9.el7.noarch 20/23

正在安装 : 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_6 21/23

正在安装 : 1:java-1.8.0-openjdk-devel-1.8.0.102-4.b14.el7.x86\_64 22/23

正在安装 : 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 23/23

development/productid | 1.6 kB 00:00

验证中 : libXext-1.3.3-3.el7.x86\_64 1/23

验证中 : 1:java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86\_64 2/23

验证中 : giflib-4.1.6-9.el7.x86\_64 3/23

验证中 : libXtst-1.2.2-2.1.el7.x86\_64 4/23

验证中 : fontpackages-filesystem-1.44-8.el7.noarch 5/23

验证中 : ttmkfdir-3.0.9-42.el7.x86\_64 6/23

验证中 : 1:java-1.8.0-openjdk-devel-1.8.0.102-4.b14.el7.x86\_64 7/23

验证中 : 1:java-1.8.0-openjdk-headless-1.8.0.102-4.b14.el7.x86\_6 8/23

验证中 : python-javapackages-3.4.1-11.el7.noarch 9/23

验证中 : libXcomposite-0.4.4-4.1.el7.x86\_64 10/23

验证中 : libXrender-0.9.8-2.1.el7.x86\_64 11/23

验证中 : lksctp-tools-1.0.17-2.el7.x86\_64 12/23

验证中 : copy-jdk-configs-1.2-1.el7.noarch 13/23

验证中 : xorg-x11-fonts-Type1-7.5-9.el7.noarch 14/23

验证中 : libXfont-1.5.1-2.el7.x86\_64 15/23

验证中 : libICE-1.0.9-2.el7.x86\_64 16/23

验证中 : javapackages-tools-3.4.1-11.el7.noarch 17/23

验证中 : tzdata-java-2016g-2.el7.noarch 18/23

验证中 : libXi-1.7.4-2.el7.x86\_64 19/23

验证中 : libSM-1.2.2-2.el7.x86\_64 20/23

验证中 : libfontenc-1.1.2-3.el7.x86\_64 21/23

验证中 : fontconfig-2.10.95-10.el7.x86\_64 22/23

验证中 : 1:xorg-x11-font-utils-7.5-20.el7.x86\_64 23/23

已安装:

java-1.8.0-openjdk.x86\_64 1:1.8.0.102-4.b14.el7

java-1.8.0-openjdk-devel.x86\_64 1:1.8.0.102-4.b14.el7

作为依赖被安装:

copy-jdk-configs.noarch 0:1.2-1.el7

fontconfig.x86\_64 0:2.10.95-10.el7

fontpackages-filesystem.noarch 0:1.44-8.el7

giflib.x86\_64 0:4.1.6-9.el7

java-1.8.0-openjdk-headless.x86\_64 1:1.8.0.102-4.b14.el7

javapackages-tools.noarch 0:3.4.1-11.el7

libICE.x86\_64 0:1.0.9-2.el7

libSM.x86\_64 0:1.2.2-2.el7

libXcomposite.x86\_64 0:0.4.4-4.1.el7

libXext.x86\_64 0:1.3.3-3.el7

libXfont.x86\_64 0:1.5.1-2.el7

libXi.x86\_64 0:1.7.4-2.el7

libXrender.x86\_64 0:0.9.8-2.1.el7

libXtst.x86\_64 0:1.2.2-2.1.el7

libfontenc.x86\_64 0:1.1.2-3.el7

lksctp-tools.x86\_64 0:1.0.17-2.el7

python-javapackages.noarch 0:3.4.1-11.el7

ttmkfdir.x86\_64 0:3.0.9-42.el7

tzdata-java.noarch 0:2016g-2.el7

xorg-x11-font-utils.x86\_64 1:7.5-20.el7

xorg-x11-fonts-Type1.noarch 0:7.5-9.el7

完毕！

[root@elk01 ~]# java -version

openjdk version "1.8.0\_102"

OpenJDK Runtime Environment (build 1.8.0\_102-b14)

OpenJDK 64-Bit Server VM (build 25.102-b14, mixed mode)

#确认环境

##安装es

#在真机上把elk的包做成yum源

[root@elk01 ~]# cat /etc/yum.repos.d/development.repo #修改yum源

[development]

name=rhel7

baseurl=ftp://192.168.4.254/pub/iso/rhel7

enabled=1

gpgcheck=0

[ELK]

name=elk

baseurl=ftp://192.168.4.254/pub/iso/elk

enabled=1

gpgcheck=0

[root@elk01 ~]# yum clean all ; yum repolist

已加载插件：langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

正在清理软件源： ELK development

Cleaning up everything

已加载插件：langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

ELK | 2.9 kB 00:00

development | 4.1 kB 00:00

(1/3): ELK/primary\_db | 12 kB 00:00

(2/3): development/group\_gz | 136 kB 00:00

(3/3): development/primary\_db | 3.9 MB 00:00

源标识 源名称 状态

ELK elk 4

development rhel7 4,751

repolist: 4,755

[root@elk01 ~]# yum -y install elasticsearch.noarch

已加载插件：langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

正在解决依赖关系

--> 正在检查事务

---> 软件包 elasticsearch.noarch.0.2.3.4-1 将被 安装

--> 解决依赖关系完成

依赖关系解决

================================================================================

Package 架构 版本 源 大小

================================================================================

正在安装:

elasticsearch noarch 2.3.4-1 ELK 26 M

事务概要

================================================================================

安装 1 软件包

总下载量：26 M

安装大小：29 M

Downloading packages:

elasticsearch-2.3.4.rpm | 26 MB 00:00

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Creating elasticsearch group... OK

Creating elasticsearch user... OK

正在安装 : elasticsearch-2.3.4-1.noarch 1/1

### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd

sudo systemctl daemon-reload

sudo systemctl enable elasticsearch.service

### You can start elasticsearch service by executing

sudo systemctl start elasticsearch.service

验证中 : elasticsearch-2.3.4-1.noarch 1/1

已安装:

elasticsearch.noarch 0:2.3.4-1

完毕！

[root@elk01 ~]# rpm -qa | grep elas

elasticsearch-2.3.4-1.noarch

[root@elk01 ~]# rpm -ql elasticsearch-2.3.4-1.noarch

/etc/elasticsearch

/etc/elasticsearch/elasticsearch.yml

/etc/elasticsearch/logging.yml

/etc/elasticsearch/scripts

/etc/init.d/elasticsearch

/etc/sysconfig/elasticsearch

/usr/lib/sysctl.d

/usr/lib/sysctl.d/elasticsearch.conf

/usr/lib/systemd/system/elasticsearch.service

/usr/lib/tmpfiles.d

/usr/lib/tmpfiles.d/elasticsearch.conf

/usr/share/elasticsearch/LICENSE.txt

/usr/share/elasticsearch/NOTICE.txt

/usr/share/elasticsearch/README.textile

/usr/share/elasticsearch/bin

/usr/share/elasticsearch/bin/elasticsearch

/usr/share/elasticsearch/bin/elasticsearch-systemd-pre-exec

/usr/share/elasticsearch/bin/elasticsearch.in.sh

/usr/share/elasticsearch/bin/plugin

/usr/share/elasticsearch/lib

/usr/share/elasticsearch/lib/HdrHistogram-2.1.6.jar

/usr/share/elasticsearch/lib/apache-log4j-extras-1.2.17.jar

/usr/share/elasticsearch/lib/commons-cli-1.3.1.jar

/usr/share/elasticsearch/lib/compiler-0.8.13.jar

/usr/share/elasticsearch/lib/compress-lzf-1.0.2.jar

/usr/share/elasticsearch/lib/elasticsearch-2.3.4.jar

/usr/share/elasticsearch/lib/guava-18.0.jar

/usr/share/elasticsearch/lib/hppc-0.7.1.jar

/usr/share/elasticsearch/lib/jackson-core-2.6.6.jar

/usr/share/elasticsearch/lib/jackson-dataformat-cbor-2.6.6.jar

/usr/share/elasticsearch/lib/jackson-dataformat-smile-2.6.6.jar

/usr/share/elasticsearch/lib/jackson-dataformat-yaml-2.6.6.jar

/usr/share/elasticsearch/lib/jna-4.1.0.jar

/usr/share/elasticsearch/lib/joda-convert-1.2.jar

/usr/share/elasticsearch/lib/joda-time-2.9.4.jar

/usr/share/elasticsearch/lib/jsr166e-1.1.0.jar

/usr/share/elasticsearch/lib/jts-1.13.jar

/usr/share/elasticsearch/lib/log4j-1.2.17.jar

/usr/share/elasticsearch/lib/lucene-analyzers-common-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-backward-codecs-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-core-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-grouping-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-highlighter-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-join-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-memory-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-misc-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-queries-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-queryparser-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-sandbox-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-spatial-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-spatial3d-5.5.0.jar

/usr/share/elasticsearch/lib/lucene-suggest-5.5.0.jar

/usr/share/elasticsearch/lib/netty-3.10.5.Final.jar

/usr/share/elasticsearch/lib/securesm-1.0.jar

/usr/share/elasticsearch/lib/snakeyaml-1.15.jar

/usr/share/elasticsearch/lib/spatial4j-0.5.jar

/usr/share/elasticsearch/lib/t-digest-3.0.jar

/usr/share/elasticsearch/modules

/usr/share/elasticsearch/modules/lang-expression

/usr/share/elasticsearch/modules/lang-expression/antlr4-runtime-4.5.1-1.jar

/usr/share/elasticsearch/modules/lang-expression/asm-5.0.4.jar

/usr/share/elasticsearch/modules/lang-expression/asm-commons-5.0.4.jar

/usr/share/elasticsearch/modules/lang-expression/lang-expression-2.3.4.jar

/usr/share/elasticsearch/modules/lang-expression/lucene-expressions-5.5.0.jar

/usr/share/elasticsearch/modules/lang-expression/plugin-descriptor.properties

/usr/share/elasticsearch/modules/lang-expression/plugin-security.policy

/usr/share/elasticsearch/modules/lang-groovy

/usr/share/elasticsearch/modules/lang-groovy/groovy-2.4.6-indy.jar

/usr/share/elasticsearch/modules/lang-groovy/lang-groovy-2.3.4.jar

/usr/share/elasticsearch/modules/lang-groovy/plugin-descriptor.properties

/usr/share/elasticsearch/modules/lang-groovy/plugin-security.policy

/usr/share/elasticsearch/modules/reindex

/usr/share/elasticsearch/modules/reindex/plugin-descriptor.properties

/usr/share/elasticsearch/modules/reindex/reindex-2.3.4.jar

/usr/share/elasticsearch/plugins

/var/lib/elasticsearch

/var/log/elasticsearch

/var/run/elasticsearch

#验证安装结果

[root@elk01 ~]# cd /etc/elasticsearch/

[root@elk01 elasticsearch]# grep -v ^# elasticsearch.yml

network.host: 0.0.0.0

http.port: 9200

[root@elk01 elasticsearch]# systemctl start elasticsearch.service

[root@elk01 elasticsearch]# systemctl enable elasticsearch.service

Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.

[root@elk01 elasticsearch]# netstat -antpu | grep java

tcp6 0 0 :::9200 :::\* LISTEN 1619/java

tcp6 0 0 :::9300 :::\* LISTEN 1619/java

[root@elk01 elasticsearch]# curl http://192.168.4.20:9200

{

"name" : "Atalon",

"cluster\_name" : "elasticsearch",

"version" : {

"number" : "2.3.4",

"build\_hash" : "e455fd0c13dceca8dbbdbb1665d068ae55dabe3f",

"build\_timestamp" : "2016-06-30T11:24:31Z",

"build\_snapshot" : false,

"lucene\_version" : "5.5.0"

},

"tagline" : "You Know, for Search"

}

##见到信息页面，服务启动成功

##配置es集群

#搭建yum

[root@es01 ~]# yum -y install java-1.8.0-openjdk-devel elasticsearch.noarch

[root@es01 ~]# grep -v ^# /etc/elasticsearch/elasticsearch.yml

cluster.name: my-elk #集群名称（任意）

node.name: es01 #节点名（主机名）

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts: ["es01", "es02", "es03", "es04"] #不必都写，最少写两个

#集群节点同步操作

[root@es02 ~]# grep -v ^# /etc/elasticsearch/elasticsearch.yml

cluster.name: my-elk

node.name: es02

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts: ["es01", "es02", "es03", "es04"]

[root@es03 ~]# grep -v ^# /etc/elasticsearch/elasticsearch.yml

cluster.name: my-elk

node.name: es03

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts: ["es01", "es02", "es03", "es04"]

[root@es04 ~]# grep -v ^# /etc/elasticsearch/elasticsearch.yml

cluster.name: my-elk

node.name: es04

network.host: 0.0.0.0

http.port: 9200

discovery.zen.ping.unicast.hosts: ["es01", "es02", "es03", "es04"]

#设置开机自启、启动服务、集群节点同步操作

[root@es01 ~]# systemctl enable elasticsearch.service

Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.

[root@es01 ~]# systemctl start elasticsearch.service

[root@es01 ~]# ss -ltunp

Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port

udp UNCONN 0 0 127.0.0.1:323 \*:\* users:(("chronyd",pid=517,fd=1))

udp UNCONN 0 0 ::1:323 :::\* users:(("chronyd",pid=517,fd=2))

tcp LISTEN 0 128 \*:111 \*:\* users:(("systemd",pid=1,fd=55))

tcp LISTEN 0 128 \*:22 \*:\* users:(("sshd",pid=745,fd=3))

tcp LISTEN 0 100 127.0.0.1:25 \*:\* users:(("master",pid=839,fd=13))

tcp LISTEN 0 128 :::111 :::\* users:(("systemd",pid=1,fd=54))

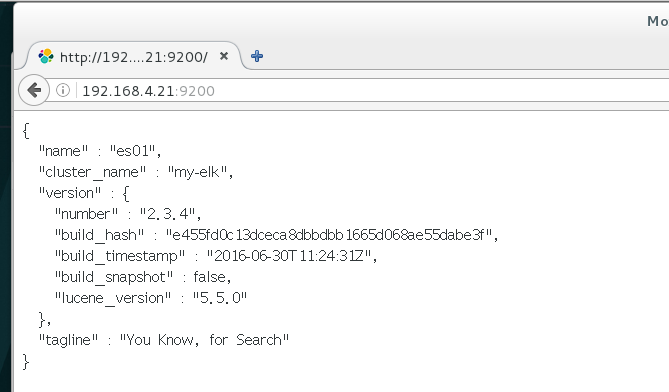
tcp LISTEN 0 50 :::9200 :::\* users:(("java",pid=1668,fd=94))

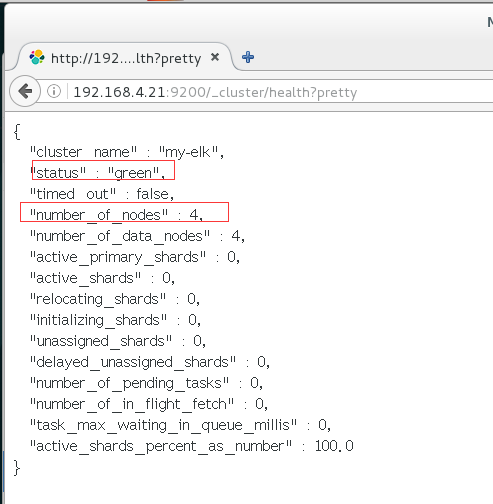
tcp LISTEN 0 50 :::9300 :::\* users:(("java",pid=1668,fd=82))

tcp LISTEN 0 128 :::22 :::\* users:(("sshd",pid=745,fd=4))

tcp LISTEN 0 100 ::1:25 :::\* users:(("master",pid=839,fd=14))

##确认监听9200/9300端口





#检查集群状态

##注意，配置文件中如果没有列出全部的集群节点，则启动顺序为先启动以标明的节点，否则比以标明节点先启动的节点会独立成单个集群，一旦出现这个情况，重启服务即可解决

##安装bigdesk、head、kopf插件

[root@es01 ~]# cd /usr/share/elasticsearch/

[root@es01 elasticsearch]# ls

bin lib LICENSE.txt modules NOTICE.txt plugins README.textile

[root@es01 bin]# ls

elasticsearch elasticsearch-systemd-pre-exec

elasticsearch.in.sh plugin

[root@es01 bin]# ./plugin --help

NAME

plugin - Manages plugins

SYNOPSIS

plugin <command>

DESCRIPTION

Manage plugins

COMMANDS

install Install a plugin

remove Remove a plugin

list List installed plugins

NOTES

[\*] For usage help on specific commands please type "plugin <command> -h"

[root@es01 bin]# ./plugin list

Installed plugins in /usr/share/elasticsearch/plugins:

- No plugin detected

[root@es01 bin]# ./plugin install <file:///tmp/bigdesk-master.zip> #注意，固定格式

-> Installing from file:/tmp/bigdesk-master.zip...

Trying file:/tmp/bigdesk-master.zip ...

Downloading ...DONE

Verifying file:/tmp/bigdesk-master.zip checksums if available ...

NOTE: Unable to verify checksum for downloaded plugin (unable to find .sha1 or .md5 file to verify)

Installed bigdesk into /usr/share/elasticsearch/plugins/bigdesk

[root@es01 bin]# ./plugin list

Installed plugins in /usr/share/elasticsearch/plugins:

- bigdesk

[root@es01 bin]# ./plugin install ftp://192.168.4.254/pub/iso/elk/elasticsearch-head-master.zip

-> Installing from ftp://192.168.4.254/pub/iso/elk/elasticsearch-head-master.zip...

Trying ftp://192.168.4.254/pub/iso/elk/elasticsearch-head-master.zip ...

Downloading .........DONE

Verifying ftp://192.168.4.254/pub/iso/elk/elasticsearch-head-master.zip checksums if available ...

Failed: IOException[sun.net.ftp.FtpProtocolException: CWD pub:550 Failed to change directory.

]; nested: FtpProtocolException[CWD pub:550 Failed to change directory.

];

NOTE: Unable to verify checksum for downloaded plugin (unable to find .sha1 or .md5 file to verify)

Installed head into /usr/share/elasticsearch/plugins/head

[root@es01 bin]# ./plugin install ftp://192.168.4.254/pub/iso/elk/elasticsearch-kopf-master.zip

-> Installing from ftp://192.168.4.254/pub/iso/elk/elasticsearch-kopf-master.zip...

Trying ftp://192.168.4.254/pub/iso/elk/elasticsearch-kopf-master.zip ...

Downloading ......................DONE

Verifying ftp://192.168.4.254/pub/iso/elk/elasticsearch-kopf-master.zip checksums if available ...

Failed: IOException[sun.net.ftp.FtpProtocolException: CWD pub:550 Failed to change directory.

]; nested: FtpProtocolException[CWD pub:550 Failed to change directory.

];

NOTE: Unable to verify checksum for downloaded plugin (unable to find .sha1 or .md5 file to verify)

Installed kopf into /usr/share/elasticsearch/plugins/kopf

[root@es01 bin]# ./plugin list

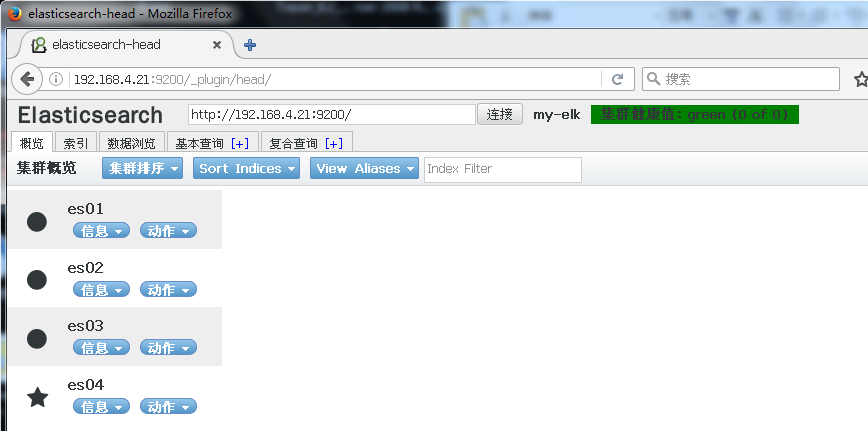
Installed plugins in /usr/share/elasticsearch/plugins:

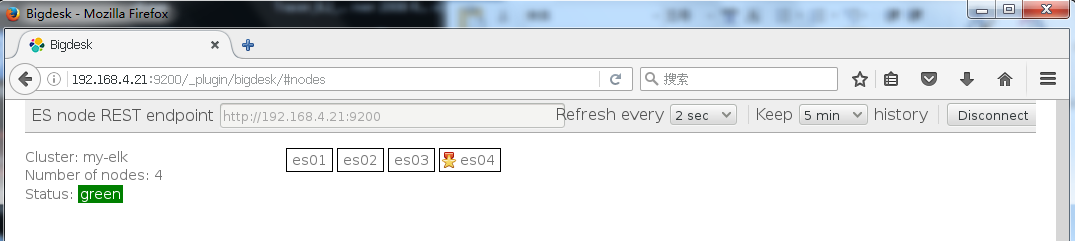
- bigdesk

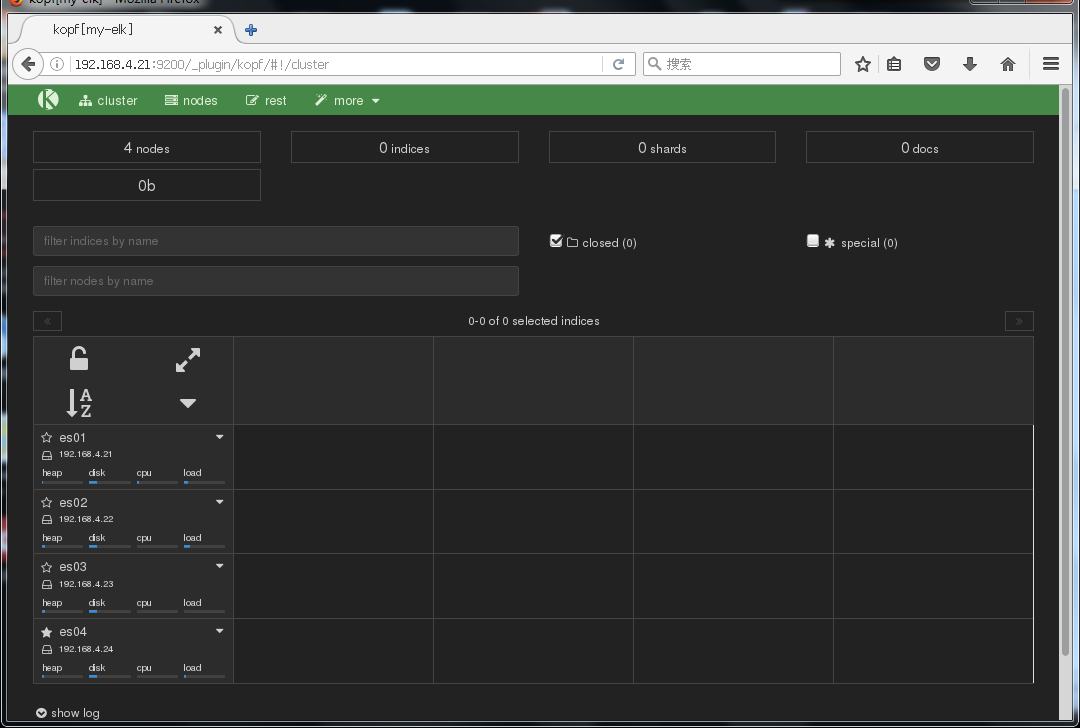
- head

- kopf

##浏览器访问







#ES-head插件：展现es集群拓扑，通过它来进行索引（index）和节点（node）级别的操作，提供一组针对集群的查询api，将结果以表和json的形式返回。提供一些快捷菜单，用以展现集群的各种状态。

#ES-kopf插件：是elasticsearch的管理工具，提供对集群操作的api

#ES-bigdesk插件：是elasticsearch的监控工具。

##操作在网页上自行联系

###补充http

#http请求方式：9种 <https://www.cnblogs.com/wan2/p/6226070.html>参照此文档

##api接口

#查询

[root@localhost ~]# curl http://192.168.4.21:9200/\_cluster/health?pretty

{

"cluster\_name" : "my-elk",

"status" : "green",

"timed\_out" : false,

"number\_of\_nodes" : 4,

"number\_of\_data\_nodes" : 4,

"active\_primary\_shards" : 4,

"active\_shards" : 12,

"relocating\_shards" : 0,

"initializing\_shards" : 0,

"unassigned\_shards" : 0,

"delayed\_unassigned\_shards" : 0,

"number\_of\_pending\_tasks" : 0,

"number\_of\_in\_flight\_fetch" : 0,

"task\_max\_waiting\_in\_queue\_millis" : 0,

"active\_shards\_percent\_as\_number" : 100.0

}

[root@localhost ~]# curl http://192.168.4.21:9200/\_cat/nodes

192.168.4.22 192.168.4.22 4 52 0.21 d m es02

192.168.4.21 192.168.4.21 4 52 0.02 d \* es01

192.168.4.23 192.168.4.23 3 51 0.00 d m es03

192.168.4.24 192.168.4.24 2 54 0.00 d m es04

[root@localhost ~]# curl http://192.168.4.21:9200/\_cat/nodes?v

host ip heap.percent ram.percent load node.role master name

192.168.4.22 192.168.4.22 4 52 0.06 d m es02

192.168.4.21 192.168.4.21 4 52 0.01 d \* es01

192.168.4.23 192.168.4.23 3 51 0.00 d m es03

192.168.4.24 192.168.4.24 2 54 0.08 d m es04

[root@localhost ~]# curl http://192.168.4.21:9200/\_cat/nodes?help

id | id,nodeId | unique node id

pid | p | process id

host | h | host name

ip | i | ip address

port | po | bound transport port

version | v | es version

build | b | es build hash

jdk | j | jdk version

disk.avail | d,disk,diskAvail | available disk space

heap.current | hc,heapCurrent | used heap

heap.percent | hp,heapPercent | used heap ratio

heap.max | hm,heapMax | max configured heap

ram.current | rc,ramCurrent | used machine memory

ram.percent | rp,ramPercent | used machine memory ratio

ram.max | rm,ramMax | total machine memory

file\_desc.current | fdc,fileDescriptorCurrent | used file descriptors

file\_desc.percent | fdp,fileDescriptorPercent | used file descriptor ratio

file\_desc.max | fdm,fileDescriptorMax | max file descriptors

cpu | cpu | recent cpu usage

load | l | most recent load avg

uptime | u | node uptime

node.role | r,role,dc,nodeRole | d:data node, c:client node

master | m | m:master-eligible, \*:current master

name | n | node name

completion.size | cs,completionSize | size of completion

fielddata.memory\_size | fm,fielddataMemory | used fielddata cache

fielddata.evictions | fe,fielddataEvictions | fielddata evictions

query\_cache.memory\_size | qcm,queryCacheMemory | used query cache

query\_cache.evictions | qce,queryCacheEvictions | query cache evictions

request\_cache.memory\_size | rcm,requestCacheMemory | used request cache

request\_cache.evictions | rce,requestCacheEvictions | request cache evictions

request\_cache.hit\_count | rchc,requestCacheHitCount | request cache hit counts

request\_cache.miss\_count | rcmc,requestCacheMissCount | request cache miss counts

flush.total | ft,flushTotal | number of flushes

flush.total\_time | ftt,flushTotalTime | time spent in flush

get.current | gc,getCurrent | number of current get ops

get.time | gti,getTime | time spent in get

get.total | gto,getTotal | number of get ops

get.exists\_time | geti,getExistsTime | time spent in successful gets

get.exists\_total | geto,getExistsTotal | number of successful gets

get.missing\_time | gmti,getMissingTime | time spent in failed gets

get.missing\_total | gmto,getMissingTotal | number of failed gets

indexing.delete\_current | idc,indexingDeleteCurrent | number of current deletions

indexing.delete\_time | idti,indexingDeleteTime | time spent in deletions

indexing.delete\_total | idto,indexingDeleteTotal | number of delete ops

indexing.index\_current | iic,indexingIndexCurrent | number of current indexing ops

indexing.index\_time | iiti,indexingIndexTime | time spent in indexing

indexing.index\_total | iito,indexingIndexTotal | number of indexing ops

indexing.index\_failed | iif,indexingIndexFailed | number of failed indexing ops

merges.current | mc,mergesCurrent | number of current merges

merges.current\_docs | mcd,mergesCurrentDocs | number of current merging docs

merges.current\_size | mcs,mergesCurrentSize | size of current merges

merges.total | mt,mergesTotal | number of completed merge ops

merges.total\_docs | mtd,mergesTotalDocs | docs merged

merges.total\_size | mts,mergesTotalSize | size merged

merges.total\_time | mtt,mergesTotalTime | time spent in merges

percolate.current | pc,percolateCurrent | number of current percolations

percolate.memory\_size | pm,percolateMemory | memory used by percolations

percolate.queries | pq,percolateQueries | number of registered percolation queries

percolate.time | pti,percolateTime | time spent percolating

percolate.total | pto,percolateTotal | total percolations

refresh.total | rto,refreshTotal | total refreshes

refresh.time | rti,refreshTime | time spent in refreshes

script.compilations | scrcc,scriptCompilations | script compilations

script.cache\_evictions | scrce,scriptCacheEvictions | script cache evictions

search.fetch\_current | sfc,searchFetchCurrent | current fetch phase ops

search.fetch\_time | sfti,searchFetchTime | time spent in fetch phase

search.fetch\_total | sfto,searchFetchTotal | total fetch ops

search.open\_contexts | so,searchOpenContexts | open search contexts

search.query\_current | sqc,searchQueryCurrent | current query phase ops

search.query\_time | sqti,searchQueryTime | time spent in query phase

search.query\_total | sqto,searchQueryTotal | total query phase ops

search.scroll\_current | scc,searchScrollCurrent | open scroll contexts

search.scroll\_time | scti,searchScrollTime | time scroll contexts held open

search.scroll\_total | scto,searchScrollTotal | completed scroll contexts

segments.count | sc,segmentsCount | number of segments

segments.memory | sm,segmentsMemory | memory used by segments

segments.index\_writer\_memory | siwm,segmentsIndexWriterMemory | memory used by index writer

segments.index\_writer\_max\_memory | siwmx,segmentsIndexWriterMaxMemory | maximum memory index writer may use before it must write buffered documents to a new segment

segments.version\_map\_memory | svmm,segmentsVersionMapMemory | memory used by version map

segments.fixed\_bitset\_memory | sfbm,fixedBitsetMemory | memory used by fixed bit sets for nested object field types and type filters for types referred in \_parent fields

suggest.current | suc,suggestCurrent | number of current suggest ops

suggest.time | suti,suggestTime | time spend in suggest

suggest.total | suto,suggestTotal | number of suggest ops

[root@localhost ~]# curl http://192.168.4.21:9200/\_cat/indices

green open bbb 4 2 0 0 1.8kb 636b

#增

[root@localhost ~]# curl -XPUT 'http://192.168.4.21:9200/school' -d '{

> "settings":{

> "index":{

> "number\_of\_shards":4,

> "number\_of\_replicas":1

> }

> }

> }'

{"acknowledged":true}[root@localhost ~]#

[root@localhost ~]# curl -XPU' -d '{

> "title": "devops",

> "name":{

> "firsh": "guzhang",

> "lsat": "wu"

> },

> "age":25}'

{"\_index":"school","\_type":"student","\_id":"1","\_version":1,"\_shards":{"total":2,"successful":2,"failed":0},"created":true}[root@localhost ~]#

#删

[root@localhost ~]# curl -XDELETE 'http://192.168.4.21:9200/aaa'

{"acknowledged":true}[root@localhost ~]#

#改

[root@localhost ~]# curl -XPOST 'http://192.168.4.21:9200/school/student/1/\_update' -d '{

"doc":{

"age":30}}'

{"\_index":"school","\_type":"student","\_id":"1","\_version":2,"\_shards":{"total":2,"successful":2,"failed":0}}[root@localhost ~]#

##批量导入

[root@localhost mnt]# gzip -d shakespeare.json.gz

[root@localhost mnt]# curl -XPOST 'http://192.168.4.21:9200/\_bulk' --data-binary @/mnt/shakespeare.json

[root@localhost mnt]# curl -XPOST 'http://192.168.4.21:9200/\_bulk' --data-binary @logs.jsonl

[root@localhost mnt]# curl -XPOST 'http://192.168.4.21:9200/accounts/act/\_bulk' --data-binary @accounts.json #无索引

##手动创建索引，然后重新导入数据

[root@localhost mnt]# curl -XPOST 'http://192.168.4.21:9200/\_bulk' --data-binary @accounts.json

##安装Logstash

#yum - y instll logstash #依赖java运行环境，需要安卓jdk-1.8.0

[root@elk01 ~]# cd /opt/logstash/bin

[root@elk01 bin]# ./

logstash logstash.lib.sh logstash-plugin plugin rspec

[root@elk01 bin]# ./logstash --help

Usage:

/bin/logstash agent [OPTIONS]

Options:

-f, --config CONFIG\_PATH Load the logstash config from a specific

or directory. If a directory is given,

files in that directory will be concaten

in lexicographical order and then parsed

single config file. You can also specify

wildcards (globs) and any matched files

be loaded in the order described above.

-e CONFIG\_STRING Use the given string as the configuratio

data. Same syntax as the config file. If

input is specified, then the following i

used as the default input:

"input { stdin { type => stdin } }"

and if no output is specified, then the

following is used as the default output:

"output { stdout { codec => rubydebug }

If you wish to use both defaults, please

the empty string for the '-e' flag.

(default: "")

-w, --pipeline-workers COUNT Sets the number of pipeline workers to r

(default: 1)

-b, --pipeline-batch-size SIZE Size of batches the pipeline is to work

(default: 125)

-u, --pipeline-batch-delay DELAY\_IN\_MS When creating pipeline batches,

for the next event.

(default: 5)

--filterworkers COUNT DEPRECATED. Now an alias for --pipeline-

-l, --log FILE Write logstash internal logs to the give

file. Without this flag, logstash will e

logs to standard output.

-v Increase verbosity of logstash internal

Specifying once will show 'informational

logs. Specifying twice will show 'debug'

logs. This flag is deprecated. You shoul

--verbose or --debug instead.

--quiet Quieter logstash logging. This causes on

errors to be emitted.

--verbose More verbose logging. This causes 'info'

level logs to be emitted.

--debug Most verbose logging. This causes 'debug

level logs to be emitted.

--debug-config Print the compiled config ruby code out

WARNING: This will include any 'passwordsult

in plaintext passwords appearing in your

(default: false)

-V, --version Emit the version of logstash and its fri

then exit.

-p, --pluginpath PATH A path of where to find plugins. This fl

can be given multiple times to include

multiple paths. Plugins are expected to

in a specific directory hierarchy:

'PATH/logstash/TYPE/NAME.rb' where TYPE

'inputs' 'filters', 'outputs' or 'codecs

and NAME is the name of the plugin.

-t, --configtest Check configuration for valid syntax and

--[no-]allow-unsafe-shutdown Force logstash to exit during shutdown e

if there are still inflight events in me

By default, logstash will refuse to quit

received events have been pushed to the

(default: false)

-r, --[no-]auto-reload Monitor configuration changes and reload

whenever it is changed.

NOTE: use SIGHUP to manually reload the

(default: false)

--reload-interval RELOAD\_INTERVAL How frequently to poll the configura

for changes, in seconds.

(default: 3)

--allow-env EXPERIMENTAL. Enables templating of envi

values. Instances of "${VAR}" in strings

with the respective environment variable

(default: false)

-h, --help print help

[root@elk01 bin]# ls

logstash logstash-plugin plugin.bat setup.bat

logstash.bat logstash-plugin.bat rspec

logstash.lib.sh plugin rspec.bat

[root@elk01 bin]# ./logstash-plugin list

Ignoring ffi-1.9.13 because its extensions are not built. Try: gem pristine ffi --version 1.9.13

logstash-codec-collectd

logstash-codec-dots

logstash-codec-edn

logstash-codec-edn\_lines

logstash-codec-es\_bulk

logstash-codec-fluent

logstash-codec-graphite

logstash-codec-json

logstash-codec-json\_lines

logstash-codec-line

logstash-codec-msgpack

logstash-codec-multiline

logstash-codec-netflow

logstash-codec-oldlogstashjson

logstash-codec-plain

logstash-codec-rubydebug

logstash-filter-anonymize

logstash-filter-checksum

logstash-filter-clone

logstash-filter-csv

logstash-filter-date

logstash-filter-dns

logstash-filter-drop

logstash-filter-fingerprint

logstash-filter-geoip

logstash-filter-grok

logstash-filter-json

logstash-filter-kv

logstash-filter-metrics

logstash-filter-multiline

logstash-filter-mutate

logstash-filter-ruby

logstash-filter-sleep

logstash-filter-split

logstash-filter-syslog\_pri

logstash-filter-throttle

logstash-filter-urldecode

logstash-filter-useragent

logstash-filter-uuid

logstash-filter-xml

logstash-input-beats

logstash-input-couchdb\_changes

logstash-input-elasticsearch

logstash-input-eventlog

logstash-input-exec

logstash-input-file

logstash-input-ganglia

logstash-input-gelf

logstash-input-generator

logstash-input-graphite

logstash-input-heartbeat

logstash-input-http

logstash-input-http\_poller

logstash-input-imap

logstash-input-irc

logstash-input-jdbc

logstash-input-kafka

logstash-input-log4j

logstash-input-lumberjack

logstash-input-pipe

logstash-input-rabbitmq

logstash-input-redis

logstash-input-s3

logstash-input-snmptrap

logstash-input-sqs

logstash-input-stdin

logstash-input-syslog

logstash-input-tcp

logstash-input-twitter

logstash-input-udp

logstash-input-unix

logstash-input-xmpp

logstash-input-zeromq

logstash-output-cloudwatch

logstash-output-csv

logstash-output-elasticsearch

logstash-output-email

logstash-output-exec

logstash-output-file

logstash-output-ganglia

logstash-output-gelf

logstash-output-graphite

logstash-output-hipchat

logstash-output-http

logstash-output-irc

logstash-output-juggernaut

logstash-output-kafka

logstash-output-lumberjack

logstash-output-nagios

logstash-output-nagios\_nsca

logstash-output-null

logstash-output-opentsdb

logstash-output-pagerduty

logstash-output-pipe

logstash-output-rabbitmq

logstash-output-redis

logstash-output-s3

logstash-output-sns

logstash-output-sqs

logstash-output-statsd

logstash-output-stdout

logstash-output-tcp

logstash-output-udp

logstash-output-xmpp

logstash-output-zeromq

logstash-patterns-core

[root@elk01 ~]# ln -s /opt/logstash/bin/logstash /usr/local/bin

[root@elk01 ~]# ln -s /opt/logstash/bin/logstash-plugin /usr/local/bin/

[root@elk01 ~]# logstash

logstash logstash-plugin

[root@elk01 ~]# logstash

[root@elk01 ~]# rpm -qa | grep logstash

logstash-2.3.4-1.noarch

[root@elk01 ~]# logstash --version

logstash 2.3.4

#编写Logstash配置文件，注意，这个配置文件需要完全手写

[root@elk01 ~]# cd /etc/logstash/

[root@elk01 logstash]# ls

conf.d

[root@elk01 logstash]# touch logstash.conf

[root@elk01 logstash]# rm -rf /usr/local/bin/logstash-plugin

[root@elk01 logstash]# alias logstash-plugin='/opt/logstash/bin/logstash-plugin'

[root@elk01 logstash]# logstash-plugin list

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

stdin{}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{}

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

ttt

2018-01-24T03:47:36.542Z elk01 ttt

date

2018-01-24T03:47:43.247Z elk01 date

##测试标准输入和标准输出

##https://github.com/logstash-plugins 帮助文档在线地址

[root@elk01 ~]# cd /etc/logstash/

[root@elk01 logstash]# vim logstash.conf

[root@elk01 logstash]# cat logstash.conf

#接受信息模块

input{

stdin{ codec => "json" }

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "json" }

}

[root@elk01 logstash]# logstash -f logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{"a":1,"b":2}

{"a":1,"b":2,"@version":"1","@timestamp":"2018-01-24T07:34:46.854Z","host":"elk01"}

[root@elk01 logstash]# cat logstash.conf

#接受信息模块

input{

stdin{ codec => "json" }

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 logstash]# logstash -f logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

abc

{

"message" => "abc",

"tags" => [

[0] "\_jsonparsefailure"

],

"@version" => "1",

"@timestamp" => "2018-01-24T07:38:03.111Z",

"host" => "elk01"

}

{"a":1,"b":2}

{

"a" => 1,

"b" => 2,

"@version" => "1",

"@timestamp" => "2018-01-24T07:41:46.566Z",

"host" => "elk01"

}

[root@elk01 logstash]# cat logstash.conf

#接受信息模块

input{

file{

path => ["/tmp/alog", "/tmp/blog" ]

type => 'filelog'

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# touch /tmp/{alog,blog}

[root@elk01 ~]# ls /tmp/\*log

/tmp/alog /tmp/blog

[root@elk01 logstash]# logstash -f logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

#再开一个终端，测试插入日志

[root@elk01 ~]# echo 12345 > /tmp/alog

{

"message" => "12345",

"@version" => "1",

"@timestamp" => "2018-01-24T08:03:26.834Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

[root@elk01 ~]# echo 67890 >> /tmp/blog

{

"message" => "67890",

"@version" => "1",

"@timestamp" => "2018-01-24T08:04:59.061Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

[root@elk01 ~]# seq 9 >> /tmp/alog

{

"message" => "1",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.182Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "2",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.184Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "3",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.208Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "4",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.210Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "5",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.216Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "6",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.216Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "7",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.234Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "8",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.234Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "9",

"@version" => "1",

"@timestamp" => "2018-01-24T08:05:32.235Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

##>和>>都会显示

#日志中有原始数据如何操作

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

path => ["/tmp/alog", "/tmp/blog" ]

type => 'filelog'

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# vim /etc/logstash/logstash.conf

[root@elk01 ~]# echo a12345 > /tmp/alog

[root@elk01 ~]# echo a12345 >> /tmp/alog

[root@elk01 ~]# echo b123456 > /tmp/blog

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

path => ["/tmp/alog", "/tmp/blog" ]

type => 'filelog'

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# cat /tmp/alog

a12345

a12345

[root@elk01 ~]# cat /tmp/blog

b123456

#重启logstash

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "a12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:22:46.341Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "a12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:22:46.644Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "b123456",

"@version" => "1",

"@timestamp" => "2018-01-24T14:22:46.652Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

#再重启logstash

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

##原因，logstash读取日志的时候会在本地硬盘生成文件指针，指针不更新，重新读取的时候不会发生数据变化

#追加数据

[root@elk01 ~]# echo c12345 >> /tmp/alog

[root@elk01 ~]# echo d12345 >> /tmp/blog

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "c12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:27:02.781Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "d12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:27:02.909Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

#验证文件指针

#日志被清空重写

[root@elk01 ~]# echo 111 > /tmp/alog

[root@elk01 ~]# echo 112 >> /tmp/alog

[root@elk01 ~]# echo 113 >> /tmp/alog

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "111",

"@version" => "1",

"@timestamp" => "2018-01-24T14:28:19.398Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "112",

"@version" => "1",

"@timestamp" => "2018-01-24T14:28:19.514Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "113",

"@version" => "1",

"@timestamp" => "2018-01-24T14:28:19.515Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

#验证文件指针

[root@elk01 ~]# echo $USER

root

[root@elk01 ~]# cat ~/.sincedb\_d1c33792769da49e7360cbdc40b675b1

5142912 0 2051 12

4588506 0 2051 15

[root@elk01 ~]# rm -rf ~/.sincedb\_d1c33792769da49e7360cbdc40b675b1

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "111",

"@version" => "1",

"@timestamp" => "2018-01-24T14:35:09.474Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "112",

"@version" => "1",

"@timestamp" => "2018-01-24T14:35:09.640Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "113",

"@version" => "1",

"@timestamp" => "2018-01-24T14:35:09.640Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "b123456",

"@version" => "1",

"@timestamp" => "2018-01-24T14:35:09.676Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "d12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:35:09.676Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

#文件指针默认放在当前用户的家目录下，是一个隐藏文件，删除后重启logstash，会从头读取日志文件

#为了避免不用用户启动logstash的时候反复重读日志文件，需要将文件指针文件改到一个公共目录

[root@elk01 ~]# vim /etc/logstash/logstash.conf

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/var/lib/logstash/sincedb-access"

path => ["/tmp/alog", "/tmp/blog" ]

type => 'filelog'

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# rm -rf ~/.sincedb\_d1c33792769da49e7360cbdc40b675b1

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "111",

"@version" => "1",

"@timestamp" => "2018-01-24T14:39:41.621Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "112",

"@version" => "1",

"@timestamp" => "2018-01-24T14:39:41.833Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "113",

"@version" => "1",

"@timestamp" => "2018-01-24T14:39:41.834Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "b123456",

"@version" => "1",

"@timestamp" => "2018-01-24T14:39:41.842Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

{

"message" => "d12345",

"@version" => "1",

"@timestamp" => "2018-01-24T14:39:41.843Z",

"path" => "/tmp/blog",

"host" => "elk01",

"type" => "filelog"

}

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

^CSIGINT received. Terminating immediately.. {:level=>:fatal}

[root@elk01 ~]# cat /var/lib/logstash/sincedb-access

5142912 0 2051 12

[root@elk01 ~]# ls ~/.sin\*

ls: 无法访问/root/.sin\*: 没有那个文件或目录

#验证修改文件指针存放目录

##tcp/udp插件

#tcp插件

[root@elk01 ~]# netstat -ltunp

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 1/systemd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 809/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 920/master

tcp6 0 0 :::111 :::\* LISTEN 1/systemd

tcp6 0 0 :::22 :::\* LISTEN 809/sshd

tcp6 0 0 ::1:25 :::\* LISTEN 920/master

udp 0 0 127.0.0.1:323 0.0.0.0:\* 538/chronyd

udp6 0 0 ::1:323 :::\* 538/chronyd

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/var/lib/logstash/sincedb-access"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

#启动logstash

[root@elk01 ~]# netstat -luntp

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 1/systemd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 809/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 920/master

tcp6 0 0 :::111 :::\* LISTEN 1/systemd

tcp6 0 0 :::9200 :::\* LISTEN 1792/java

tcp6 0 0 :::9300 :::\* LISTEN 1792/java

tcp6 0 0 :::22 :::\* LISTEN 809/sshd

tcp6 0 0 :::8888 :::\* LISTEN 1898/java

tcp6 0 0 ::1:25 :::\* LISTEN 920/master

udp 0 0 127.0.0.1:323 0.0.0.0:\* 538/chronyd

udp6 0 0 ::1:323 :::\* 538/chronyd

#监听到8888端口

##客户端测试

#python脚本测试

[root@localhost ~]# cat send.py

#!/usr/bin/env python

import socket, sys

def sendmsg(msg):

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM, socket.IPPROTO\_TCP)

s.connect(("192.168.4.20", 8888))

s.sendall(msg)

s.close

sendmsg(sys.argv[1])

[root@localhost ~]# python send.py 'abcd

{

"message" => "abcd",

"@version" => "1",

"@timestamp" => "2018-01-24T15:46:26.386Z",

"host" => "192.168.4.254",

"port" => 55964,

"type" => "tcplog"

}

#监听端确认收到tcp信息

#shell脚本测试

[root@localhost ~]# cat send.sh

#!/bin/bash

function sendmsg(){

exec 9<>/dev/tcp/192.168.4.20/8888

exec 5>&1 >&9

echo "$1"

exec >&5

exec 5>&- 9>&-

}

sendmsg "$1"

#shell脚本这么写我也看不懂。。。。。。

[root@localhost ~]# bash send.sh "abcd"

[root@localhost ~]# bash send.sh "is shell"

{

"message" => "abcd",

"@version" => "1",

"@timestamp" => "2018-01-24T15:55:50.207Z",

"host" => "192.168.4.254",

"port" => 55970,

"type" => "tcplog"

}

{

"message" => "is shell",

"@version" => "1",

"@timestamp" => "2018-01-24T15:55:59.528Z",

"host" => "192.168.4.254",

"port" => 55972,

"type" => "tcplog"

}

#监听端收到tcp消息

#用curl工具测试

[root@localhost ~]# curl -m 1 http://192.168.4.20:8888

curl: (28) Operation timed out after 1003 milliseconds with 0 out of -1 bytes received

{

"message" => "GET / HTTP/1.1\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:03:32.287Z",

"host" => "192.168.4.254",

"port" => 55974,

"type" => "tcplog"

}

{

"message" => "User-Agent: curl/7.29.0\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:03:32.288Z",

"host" => "192.168.4.254",

"port" => 55974,

"type" => "tcplog"

}

{

"message" => "Host: 192.168.4.20:8888\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:03:32.291Z",

"host" => "192.168.4.254",

"port" => 55974,

"type" => "tcplog"

}

{

"message" => "Accept: \*/\*\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:03:32.292Z",

"host" => "192.168.4.254",

"port" => 55974,

"type" => "tcplog"

}

{

"message" => "\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:03:32.306Z",

"host" => "192.168.4.254",

"port" => 55974,

"type" => "tcplog"

}

#udp插件

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/var/lib/logstash/sincedb-access"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# netstat -luntp

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 1/systemd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 809/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 920/master

tcp6 0 0 :::111 :::\* LISTEN 1/systemd

tcp6 0 0 :::9200 :::\* LISTEN 1792/java

tcp6 0 0 :::9300 :::\* LISTEN 1792/java

tcp6 0 0 :::22 :::\* LISTEN 809/sshd

tcp6 0 0 :::8888 :::\* LISTEN 2124/java

tcp6 0 0 ::1:25 :::\* LISTEN 920/master

udp 0 0 127.0.0.1:323 0.0.0.0:\* 538/chronyd

udp6 0 0 :::9999 :::\* 2124/java

udp6 0 0 ::1:323 :::\* 538/chronyd

#确认监听udp的9999端口

#采用iptables端口重定向的方式进行测试

[root@elk01 ~]# iptables -t nat -A PREROUTING -d 192.168.4.20 -p udp --dport 53 -j REDIRECT --to 9999

[root@localhost ~]# dig -p 9999 @192.168.4.20 A www.baidu.com

; <<>> DiG 9.9.4-RedHat-9.9.4-37.el7 <<>> -p 9999 @192.168.4.20 A www.baidu.com

; (1 server found)

;; global options: +cmd

;; connection timed out; no servers could be reached

{

"message" => "\u0012B\u0001 \u0000\u0001\u0000\u0000\u0000\u0000\u0000\u0001\u0003www\u0005baidu\u0003com\u0000\u0000\u0001\u0000\u0001\u0000\u0000)\u0010\u0000\u0000\u0000\u0000\u0000\u0000\u0000",

"@version" => "1",

"@timestamp" => "2018-01-24T16:19:31.977Z",

"type" => "udplog",

"host" => "192.168.4.254"

}

{

"message" => "\u0012B\u0001 \u0000\u0001\u0000\u0000\u0000\u0000\u0000\u0001\u0003www\u0005baidu\u0003com\u0000\u0000\u0001\u0000\u0001\u0000\u0000)\u0010\u0000\u0000\u0000\u0000\u0000\u0000\u0000",

"@version" => "1",

"@timestamp" => "2018-01-24T16:19:36.969Z",

"type" => "udplog",

"host" => "192.168.4.254"

}

{

"message" => "\u0012B\u0001 \u0000\u0001\u0000\u0000\u0000\u0000\u0000\u0001\u0003www\u0005baidu\u0003com\u0000\u0000\u0001\u0000\u0001\u0000\u0000)\u0010\u0000\u0000\u0000\u0000\u0000\u0000\u0000",

"@version" => "1",

"@timestamp" => "2018-01-24T16:19:41.970Z",

"type" => "udplog",

"host" => "192.168.4.254"

}

#确认监控端收到udp请求消息

#shell脚本测试udp信息

[root@localhost ~]# bash sendudp.sh "1234"

[root@localhost ~]# cat sendudp.sh

#!/bin/bash

function sendudp(){

exec 9<>/dev/udp/192.168.4.20/9999

echo -ne "$1\r" >&9

exec 9<&-

}

sendudp "$1

{

"message" => "1234\r",

"@version" => "1",

"@timestamp" => "2018-01-24T16:57:54.732Z",

"type" => "udplog",

"host" => "192.168.4.254"

}

#监控端接收到udp请求消息

##syslog插件

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/var/lib/logstash/sincedb-access"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# netstat -luntp

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 1/systemd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 809/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 920/master

tcp6 0 0 :::111 :::\* LISTEN 1/systemd

tcp6 0 0 :::9200 :::\* LISTEN 1792/java

tcp6 0 0 :::9300 :::\* LISTEN 1792/java

tcp6 0 0 :::22 :::\* LISTEN 809/sshd

tcp6 0 0 :::8888 :::\* LISTEN 2237/java

tcp6 0 0 ::1:25 :::\* LISTEN 920/master

tcp6 0 0 192.168.4.20:514 :::\* LISTEN 2237/java

udp 0 0 127.0.0.1:323 0.0.0.0:\* 538/chronyd

udp6 0 0 :::9999 :::\* 2237/java

udp6 0 0 ::1:323 :::\* 538/chronyd

udp6 0 0 192.168.4.20:514 :::\* 2237/java

#确认监听514端口

[root@localhost ~]# sed -n '75p' /etc/rsyslog.conf

local0.info @@192.168.4.20:514

[root@localhost ~]# systemctl restart rsyslog.service

#修改客户端syslog配置

[root@localhost ~]# logger -p local0.info -t test "test send log"

[root@localhost ~]# tail -5 /var/log/messages

Jan 25 00:45:37 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.7" x-pid="21954" x-info="http://www.rsyslog.com"] exiting on signal 15.

Jan 25 00:45:37 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.7" x-pid="22095" x-info="http://www.rsyslog.com"] start

Jan 25 00:45:37 localhost systemd: Starting System Logging Service...

Jan 25 00:45:37 localhost systemd: Started System Logging Service.

Jan 25 00:45:48 localhost test: test send log

#测试local0.info日志

{

"message" => "test send log\n",

"@version" => "1",

"@timestamp" => "2018-01-24T16:45:48.000Z",

"type" => "syslog",

"host" => "192.168.4.254",

"priority" => 134,

"timestamp" => "Jan 25 00:45:48",

"logsource" => "localhost",

"program" => "test",

"severity" => 6,

"facility" => 16,

"facility\_label" => "local0",

"severity\_label" => "Informational"

}

#本地有记录且监控端有信息记录

[root@localhost ~]# logger -p local7.info -t test "test send log"

[root@localhost ~]# tail -5 /var/log/messages

Jan 25 00:45:37 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.7" x-pid="22095" x-info="http://www.rsyslog.com"] start

Jan 25 00:45:37 localhost systemd: Starting System Logging Service...

Jan 25 00:45:37 localhost systemd: Started System Logging Service.

Jan 25 00:45:48 localhost test: test send log

Jan 25 00:46:14 localhost test: test send log

#测试local7.info日志

#本地有记录监控端无记录

##grok插件使用

[root@elk01 ~]# ls

alog.gz anaconda-ks.cfg data.rar rar rarlinux-x64-5.5.0.tar.gz

[root@elk01 ~]# gzip -d alog.gz

[root@elk01 ~]# ls

alog anaconda-ks.cfg data.rar rar rarlinux-x64-5.5.0.tar.gz

[root@elk01 ~]# cat /tmp/alog

220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] "GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1" 200 20756 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)" "-" zxzs.buildhr.com 558742

#截取加强apache日志到alog，logstash配置延续之前的配置

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:13:20.914Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

#启动logstash，查看日志信息

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{ }

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:16:35.480Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog"

}

#调试技巧，将指针文件放到/dev/null，每次启动logstash都从头读取日志文件

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => []

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:22:00.006Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"tags" => [

[0] "\_grokparsefailure"

]

}

#一次匹配

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => ["message","(?<key>reg)"]

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:27:20.866Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"tags" => [

[0] "\_grokparsefailure"

]

}

#二次匹配

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => ["message","(?<ipaddr>([12]?\d?\d\.){3}([12]?\d?\d))"]

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:33:56.002Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"ipaddr" => "220.181.108.115"

}

#三次匹配，拿到ipaddr

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => ["message","(?<ipaddr>([12]?\d?\d\.){3}([12]?\d?\d)) \S+ \S+ (?<time>.\*\])\s+\"(?<method>[A-Z]+)"]

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:43:21.426Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"ipaddr" => "220.181.108.115",

"time" => "[11/Jul/2017:03:07:16 +0800]",

"method" => "GET"

}

#四次匹配

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => ["message","(?<ipaddr>([12]?\d?\d\.){3}([12]?\d?\d)) \S+ \S+ (?<time>.\*\])\s+\"(?<method>[A-Z]+) (?<URL>/\S+)"]

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:51:38.178Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"ipaddr" => "220.181.108.115",

"time" => "[11/Jul/2017:03:07:16 +0800]",

"method" => "GET",

"URL" => "/%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html"

}

#五次匹配

[root@elk01 ~]# cd /opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns/

[root@elk01 patterns]# ls

aws exim haproxy linux-syslog mongodb rails

bacula firewalls java mcollective nagios redis

bro grok-patterns junos mcollective-patterns postgresql ruby

#正则表达式的宏 grok-patterns

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

match => ["message","%{IP:ip}"]

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "220.181.108.115 - - [11/Jul/2017:03:07:16 +0800] \"GET /%B8%DF%BC%B6%D7%E2%C1%DE%D6%F7%C8%CE/QYQiu\_j.html HTTP/1.1\" 200 20756 \"-\" \"Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)\" \"-\" zxzs.buildhr.com 558742",

"@version" => "1",

"@timestamp" => "2018-01-24T17:59:04.779Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"ip" => "220.181.108.115"

}

#调用宏匹配IP地址

#拷贝本机apache的正常访问日志到/tmp/alog,测试grok正则表达式的apache宏

#至于怎么造日志，自己研究，apache的日志

[root@elk01 ~]# cat /tmp/alog

192.168.4.20 - - [25/Jan/2018:10:17:37 +0800] "GET / HTTP/1.1" 200 10 "-" "curl/7.29.0"

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

grok{

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

}

}

#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# logstash -f /etc/logstash/

Settings: Default pipeline workers: 1

Pipeline main started

{

"message" => "192.168.4.20 - - [25/Jan/2018:10:17:37 +0800] \"GET / HTTP/1.1\" 200 10 \"-\" \"curl/7.29.0\"",

"@version" => "1",

"@timestamp" => "2018-01-25T02:44:35.434Z",

"path" => "/tmp/alog",

"host" => "elk01",

"type" => "filelog",

"clientip" => "192.168.4.20",

"ident" => "-",

"auth" => "-",

"timestamp" => "25/Jan/2018:10:17:37 +0800",

"verb" => "GET",

"request" => "/",

"httpversion" => "1.1",

"response" => "200",

"bytes" => "10"

}

##grok宏位置

[root@elk01 ~]# cd /opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.5/patterns/

[root@elk01 patterns]# ls

aws exim haproxy linux-syslog mongodb rails

bacula firewalls java mcollective nagios redis

bro grok-patterns junos mcollective-patterns postgresql ruby

[root@elk01 patterns]# vim grok-patterns

#匹配APACHE，有两个选项，一个是正确日志，一个是错误日志

##json格式的日志

#匹配奇数行

[root@elk01 ~]# awk '{if(NR%2)print $0}' logs.jsonl | wc -l

14005

#重定向偶数行

[root@elk01 ~]# sed -n '0~2p' logs.jsonl > weblog

[root@elk01 ~]# tail -n 1 weblog > /tmp/alog

[root@elk01 ~]# cat /tmp/alog

{"@timestamp":"2015-05-20T14:46:52.269Z","ip":"134.161.64.242","extension":"css","response":"200","geo":{"coordinates":{"lat":62.64858333,"lon":-160.1898889},"src":"US","dest":"CS","srcdest":"US:CS"},"@tags":["warning","info"],"utc\_time":"2015-05-20T14:46:52.269Z","referer":"http://www.slate.com/error/andr-kuipers","agent":"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1","clientip":"134.161.64.242","bytes":4116,"host":"cdn.theacademyofperformingartsandscience.org","request":"/styles/ad-blocker.css","url":"https://cdn.theacademyofperformingartsandscience.org/styles/ad-blocker.css","@message":"134.161.64.242 - - [2015-05-20T14:46:52.269Z] \"GET /styles/ad-blocker.css HTTP/1.1\" 200 4116 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"","spaces":"this is a thing with lots of spaces wwwwoooooo","xss":"<script>console.log(\"xss\")</script>","headings":["<h3>albert-sacco</h5>","http://www.slate.com/success/carlos-i-noriega"],"links":["maksim-surayev@twitter.com","http://twitter.com/login/liu-wang","www.www.slate.com"],"relatedContent":[{"url":"http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954","og:type":"article","og:title":"Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1","og:description":"Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...","og:url":"http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954","article:published\_time":"2008-03-03T15:45:41-08:00","article:modified\_time":"2014-11-27T10:00:32-08:00","article:section":"Music","og:image":"http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg","og:image:height":"723","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1","twitter:description":"Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936","og:type":"article","og:title":"&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4","og:description":"Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...","og:url":"http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936","article:published\_time":"2008-03-06T11:00:00-08:00","article:modified\_time":"2014-11-27T06:47:46-08:00","article:section":"Music","article:tag":"Donald Judd","og:image":"http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg","og:image:height":"468","og:image:width":"535","og:site\_name":"LA Weekly","twitter:title":"&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4","twitter:description":"Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738","og:type":"article","og:title":"Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08","og:description":"Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...","og:url":"http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738","article:published\_time":"2008-01-22T09:07:07-08:00","article:modified\_time":"2014-11-27T06:47:35-08:00","article:section":"Music","article:tag":"Jonny Bell","og:image":"http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg","og:image:height":"359","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08","twitter:description":"Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...","twitter:card":"summary","twitter:image":"http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/music/black-rock-city-hit-parade-2409397","og:type":"article","og:title":"Black Rock City Hit Parade","og:description":"By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...","og:url":"http://www.laweekly.com/music/black-rock-city-hit-parade-2409397","article:published\_time":"2007-08-31T13:41:39-07:00","article:modified\_time":"2014-11-27T09:41:10-08:00","article:section":"Music","og:site\_name":"LA Weekly","twitter:title":"Black Rock City Hit Parade","twitter:description":"By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...","twitter:card":"summary","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568","og:type":"article","og:title":"Calvin Harris, Henry Fonda, 4/23","og:description":"Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...","og:url":"http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568","article:published\_time":"2008-04-24T08:45:07-07:00","article:modified\_time":"2014-11-27T08:57:00-08:00","article:section":"Music","article:tag":"Timothy Norris","og:image":"http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg","og:image:height":"319","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Calvin Harris, Henry Fonda, 4/23","twitter:description":"Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg","twitter:site":"@laweekly"}],"machine":{"os":"win 8","ram":4294967296},"@version":"1"}

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

codec => "json"

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

}

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"@timestamp" => "2015-05-20T14:46:52.269Z",

"ip" => "134.161.64.242",

"extension" => "css",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 62.64858333,

"lon" => -160.1898889

},

"src" => "US",

"dest" => "CS",

"srcdest" => "US:CS"

},

"@tags" => [

[0] "warning",

[1] "info"

],

"utc\_time" => "2015-05-20T14:46:52.269Z",

"referer" => "http://www.slate.com/error/andr-kuipers",

"agent" => "Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",

"clientip" => "134.161.64.242",

"bytes" => 4116,

"host" => "cdn.theacademyofperformingartsandscience.org",

"request" => "/styles/ad-blocker.css",

"url" => "https://cdn.theacademyofperformingartsandscience.org/styles/ad-blocker.css",

"@message" => "134.161.64.242 - - [2015-05-20T14:46:52.269Z] \"GET /styles/ad-blocker.css HTTP/1.1\" 200 4116 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>albert-sacco</h5>",

[1] "http://www.slate.com/success/carlos-i-noriega"

],

"links" => [

[0] "maksim-surayev@twitter.com",

[1] "http://twitter.com/login/liu-wang",

[2] "www.www.slate.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"og:type" => "article",

"og:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"og:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"og:url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"article:published\_time" => "2008-03-03T15:45:41-08:00",

"article:modified\_time" => "2014-11-27T10:00:32-08:00",

"article:section" => "Music",

"og:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"og:image:height" => "723",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"twitter:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"twitter:site" => "@laweekly"

},

[1] {

"url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"og:type" => "article",

"og:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"og:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"og:url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"article:published\_time" => "2008-03-06T11:00:00-08:00",

"article:modified\_time" => "2014-11-27T06:47:46-08:00",

"article:section" => "Music",

"article:tag" => "Donald Judd",

"og:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"og:image:height" => "468",

"og:image:width" => "535",

"og:site\_name" => "LA Weekly",

"twitter:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"twitter:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"twitter:site" => "@laweekly"

},

[2] {

"url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"og:type" => "article",

"og:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"og:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"og:url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"article:published\_time" => "2008-01-22T09:07:07-08:00",

"article:modified\_time" => "2014-11-27T06:47:35-08:00",

"article:section" => "Music",

"article:tag" => "Jonny Bell",

"og:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"og:image:height" => "359",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"twitter:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"twitter:site" => "@laweekly"

},

[3] {

"url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"og:type" => "article",

"og:title" => "Black Rock City Hit Parade",

"og:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"og:url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"article:published\_time" => "2007-08-31T13:41:39-07:00",

"article:modified\_time" => "2014-11-27T09:41:10-08:00",

"article:section" => "Music",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Black Rock City Hit Parade",

"twitter:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

},

[4] {

"url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"og:type" => "article",

"og:title" => "Calvin Harris, Henry Fonda, 4/23",

"og:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"og:url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"article:published\_time" => "2008-04-24T08:45:07-07:00",

"article:modified\_time" => "2014-11-27T08:57:00-08:00",

"article:section" => "Music",

"article:tag" => "Timothy Norris",

"og:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"og:image:height" => "319",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Calvin Harris, Henry Fonda, 4/23",

"twitter:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "win 8",

"ram" => 4294967296

},

"@version" => "1",

"path" => "/tmp/alog",

"type" => "filelog"

}

#启动logstash，确认处理结果

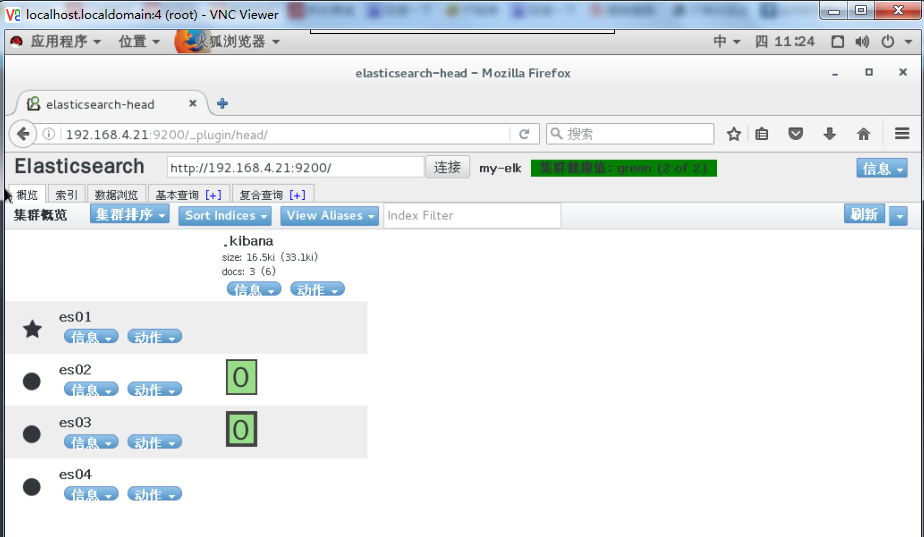
#信息输出模块

output{

stdout{ codec => "rubydebug" }

}

##将日志存入es集群



#确认集群状态

[root@elk01 ~]# > /tmp/alog

[root@elk01 ~]# cat /tmp/alog

#清空alog文件

#启动logstash监控

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

codec => "json"

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

}

#信息输出模块

output{

if [type] == "filelog"{

elasticsearch {

hosts => ["192.168.4.21:9200", "192.168.4.22:9200"]

index => "weblog"

flush\_size => 2000

idle\_flush\_time => 10

}

}

}

#启动输出模块

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

#启动监控端，显示为空

#用python的方式写入日志

[root@elk01 ~]# python

Python 2.7.5 (default, Aug 2 2016, 04:20:16)

[GCC 4.8.5 20150623 (Red Hat 4.8.5-4)] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> sfd = open("/root/weblog", "rb")

>>> dfd = open("/tmp/alog", "ab+")

>>> log = sfd.readline()

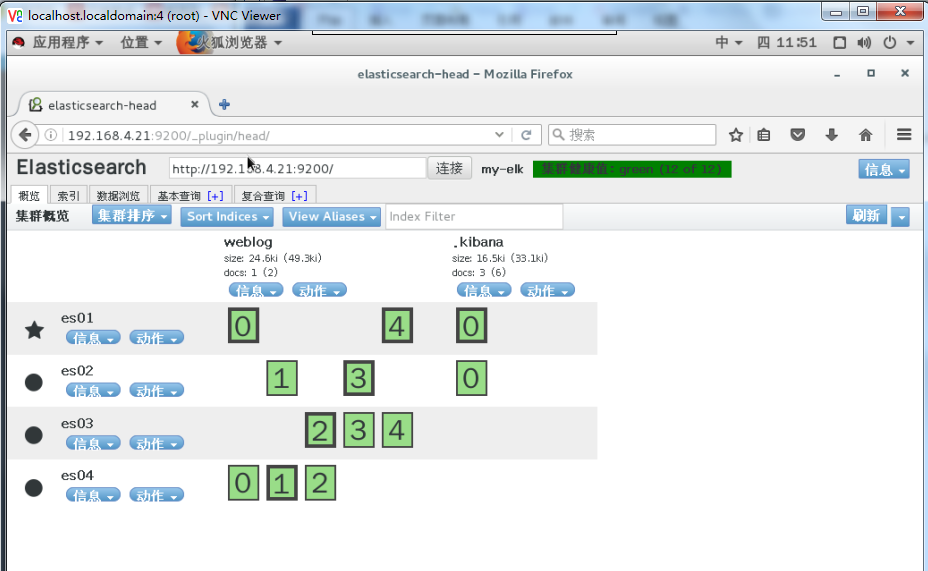
>>> dfd.write(log)

>>> exit()

[root@elk01 ~]# cat /tmp/alog

{"@timestamp":"2015-05-18T09:03:25.877Z","ip":"185.124.182.126","extension":"gif","response":"404","geo":{"coordinates":{"lat":36.518375,"lon":-86.05828083},"src":"PH","dest":"MM","srcdest":"PH:MM"},"@tags":["success","info"],"utc\_time":"2015-05-18T09:03:25.877Z","referer":"http://twitter.com/error/william-shepherd","agent":"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1","clientip":"185.124.182.126","bytes":804,"host":"motion-media.theacademyofperformingartsandscience.org","request":"/canhaz/gemini-7.gif","url":"https://motion-media.theacademyofperformingartsandscience.org/canhaz/gemini-7.gif","@message":"185.124.182.126 - - [2015-05-18T09:03:25.877Z] \"GET /canhaz/gemini-7.gif HTTP/1.1\" 404 804 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"","spaces":"this is a thing with lots of spaces wwwwoooooo","xss":"<script>console.log(\"xss\")</script>","headings":["<h3>f-i-j-nl-ng</h5>","http://facebook.com/success/lodewijk-van-den-berg"],"links":["daniel-tani@facebook.com","http://nytimes.com/security/kathryn-sullivan","www.nytimes.com"],"relatedContent":[{"url":"http://www.laweekly.com/news/cbs-crew-rat-fink-2368032","og:type":"article","og:title":"CBS Crew Rat Fink","og:description":"Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...","og:url":"http://www.laweekly.com/news/cbs-crew-rat-fink-2368032","article:published\_time":"2008-01-14T08:05:26-08:00","article:modified\_time":"2014-10-28T14:59:52-07:00","article:section":"News","article:tag":"Mark Mauer","og:image":"http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"CBS Crew Rat Fink","twitter:description":"Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043","og:type":"article","og:title":"Push and Retna in Koreatown","og:description":"Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...","og:url":"http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043","article:published\_time":"2008-01-29T07:28:32-08:00","article:modified\_time":"2014-10-28T14:59:54-07:00","article:section":"News","article:tag":"Shelley Leopold","og:image":"http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Push and Retna in Koreatown","twitter:description":"Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012","og:type":"article","og:title":"Asylm, Ruets, PDB on Santa Monica","og:description":"Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...","og:url":"http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012","article:published\_time":"2008-04-22T15:11:15-07:00","article:modified\_time":"2014-10-28T14:59:48-07:00","article:section":"News","article:tag":"Culture and Lifestyle","og:image":"http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Asylm, Ruets, PDB on Santa Monica","twitter:description":"Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...","twitter:card":"summary","twitter:image":"http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867","og:type":"article","og:title":"Laurence Tribe Tangles with CBS and L.A. City Hall","og:description":"The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...","og:url":"http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867","article:published\_time":"2008-06-04T14:16:10-07:00","article:modified\_time":"2014-11-26T14:43:59-08:00","article:section":"News","og:site\_name":"LA Weekly","twitter:title":"Laurence Tribe Tangles with CBS and L.A. City Hall","twitter:description":"The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...","twitter:card":"summary","twitter:site":"@laweekly"}],"machine":{"os":"win xp","ram":3221225472},"@version":"1"}

#刷新监控页面，数据写入



#循环写入数据

[root@elk01 ~]# python

Python 2.7.5 (default, Aug 2 2016, 04:20:16)

[GCC 4.8.5 20150623 (Red Hat 4.8.5-4)] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> rfd = open("/root/weblog", "rb")

>>> wfd = open("/tmp/alog", "ab+")

>>> rfd.readline()

'{"@timestamp":"2015-05-18T09:03:25.877Z","ip":"185.124.182.126","extension":"gif","response":"404","geo":{"coordinates":{"lat":36.518375,"lon":-86.05828083},"src":"PH","dest":"MM","srcdest":"PH:MM"},"@tags":["success","info"],"utc\_time":"2015-05-18T09:03:25.877Z","referer":"http://twitter.com/error/william-shepherd","agent":"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1","clientip":"185.124.182.126","bytes":804,"host":"motion-media.theacademyofperformingartsandscience.org","request":"/canhaz/gemini-7.gif","url":"https://motion-media.theacademyofperformingartsandscience.org/canhaz/gemini-7.gif","@message":"185.124.182.126 - - [2015-05-18T09:03:25.877Z] \\"GET /canhaz/gemini-7.gif HTTP/1.1\\" 404 804 \\"-\\" \\"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\\"","spaces":"this is a thing with lots of spaces wwwwoooooo","xss":"<script>console.log(\\"xss\\")</script>","headings":["<h3>f-i-j-nl-ng</h5>","http://facebook.com/success/lodewijk-van-den-berg"],"links":["daniel-tani@facebook.com","http://nytimes.com/security/kathryn-sullivan","www.nytimes.com"],"relatedContent":[{"url":"http://www.laweekly.com/news/cbs-crew-rat-fink-2368032","og:type":"article","og:title":"CBS Crew Rat Fink","og:description":"Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...","og:url":"http://www.laweekly.com/news/cbs-crew-rat-fink-2368032","article:published\_time":"2008-01-14T08:05:26-08:00","article:modified\_time":"2014-10-28T14:59:52-07:00","article:section":"News","article:tag":"Mark Mauer","og:image":"http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"CBS Crew Rat Fink","twitter:description":"Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043","og:type":"article","og:title":"Push and Retna in Koreatown","og:description":"Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...","og:url":"http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043","article:published\_time":"2008-01-29T07:28:32-08:00","article:modified\_time":"2014-10-28T14:59:54-07:00","article:section":"News","article:tag":"Shelley Leopold","og:image":"http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Push and Retna in Koreatown","twitter:description":"Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...","twitter:card":"summary","twitter:image":"http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012","og:type":"article","og:title":"Asylm, Ruets, PDB on Santa Monica","og:description":"Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...","og:url":"http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012","article:published\_time":"2008-04-22T15:11:15-07:00","article:modified\_time":"2014-10-28T14:59:48-07:00","article:section":"News","article:tag":"Culture and Lifestyle","og:image":"http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg","og:image:height":"360","og:image:width":"480","og:site\_name":"LA Weekly","twitter:title":"Asylm, Ruets, PDB on Santa Monica","twitter:description":"Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...","twitter:card":"summary","twitter:image":"http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg","twitter:site":"@laweekly"},{"url":"http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867","og:type":"article","og:title":"Laurence Tribe Tangles with CBS and L.A. City Hall","og:description":"The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...","og:url":"http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867","article:published\_time":"2008-06-04T14:16:10-07:00","article:modified\_time":"2014-11-26T14:43:59-08:00","article:section":"News","og:site\_name":"LA Weekly","twitter:title":"Laurence Tribe Tangles with CBS and L.A. City Hall","twitter:description":"The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...","twitter:card":"summary","twitter:site":"@laweekly"}],"machine":{"os":"win xp","ram":3221225472},"@version":"1"}\n'

>>> for i in rfd:

... wfd.write(i)

...

>>>exit()

#启动kibana服务

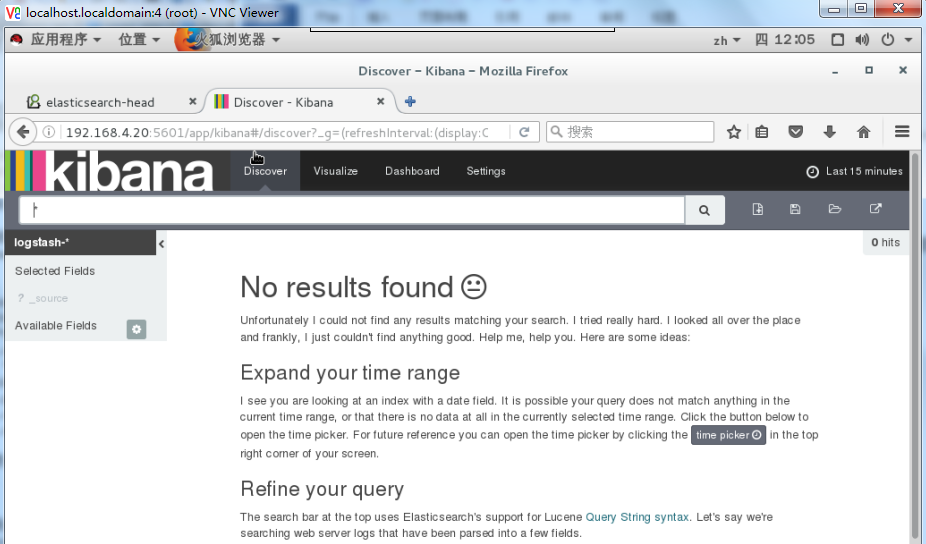
[root@elk01 ~]# systemctl enable kibana.service

Created symlink from /etc/systemd/system/multi-user.target.wants/kibana.service to /usr/lib/systemd/system/kibana.service.

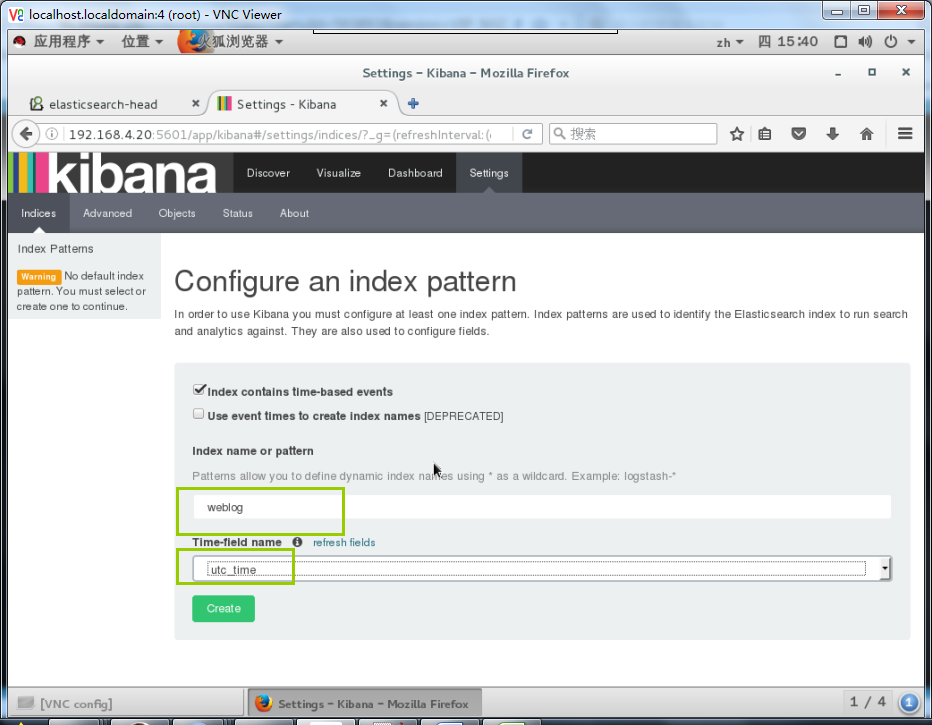
[root@elk01 ~]# systemctl restart kibana.service

[root@elk01 ~]# netstat -antpu | grep :5601

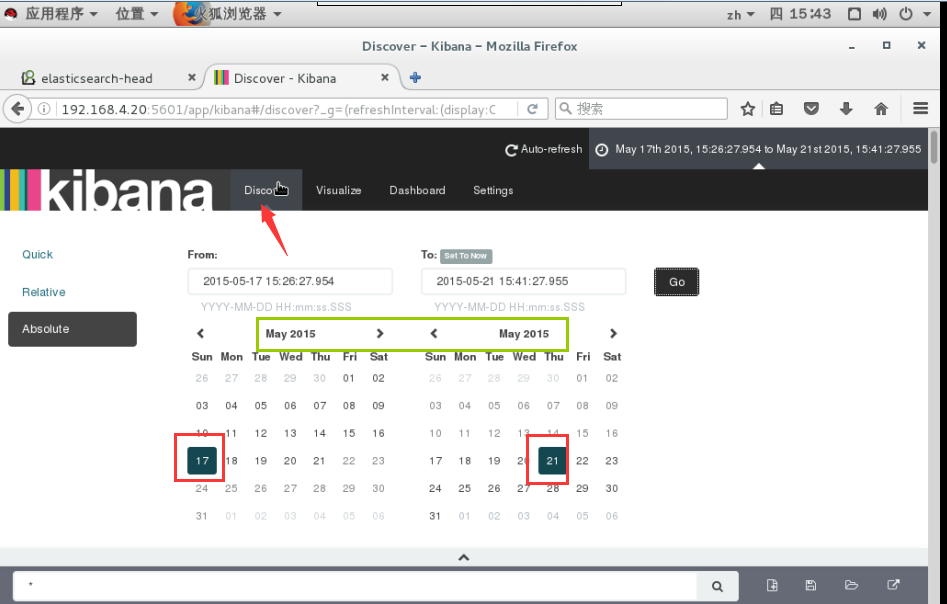
tcp 0 0 0.0.0.0:5601 0.0.0.0:\* LISTEN 3841/node

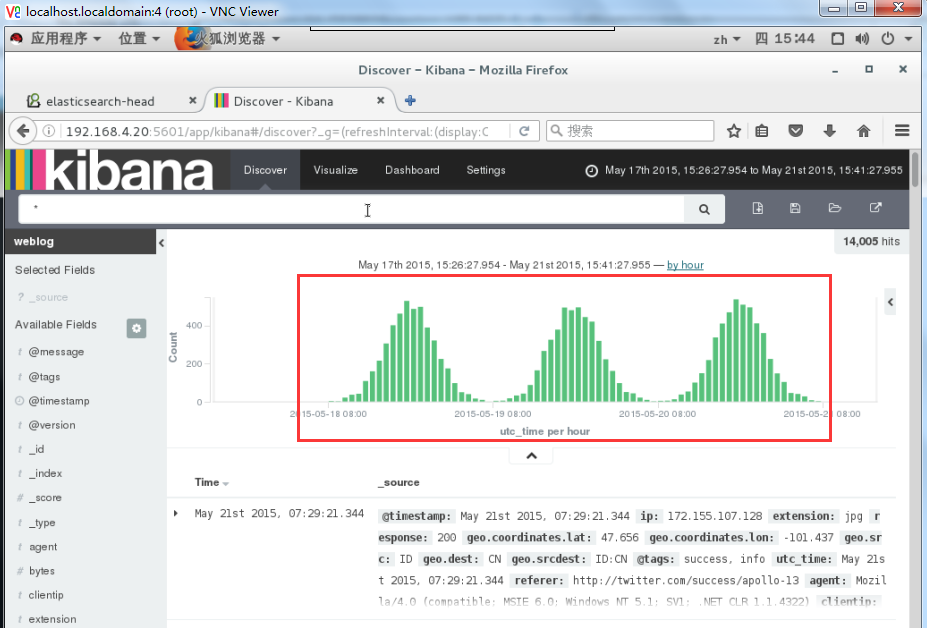


#访问kibana页面

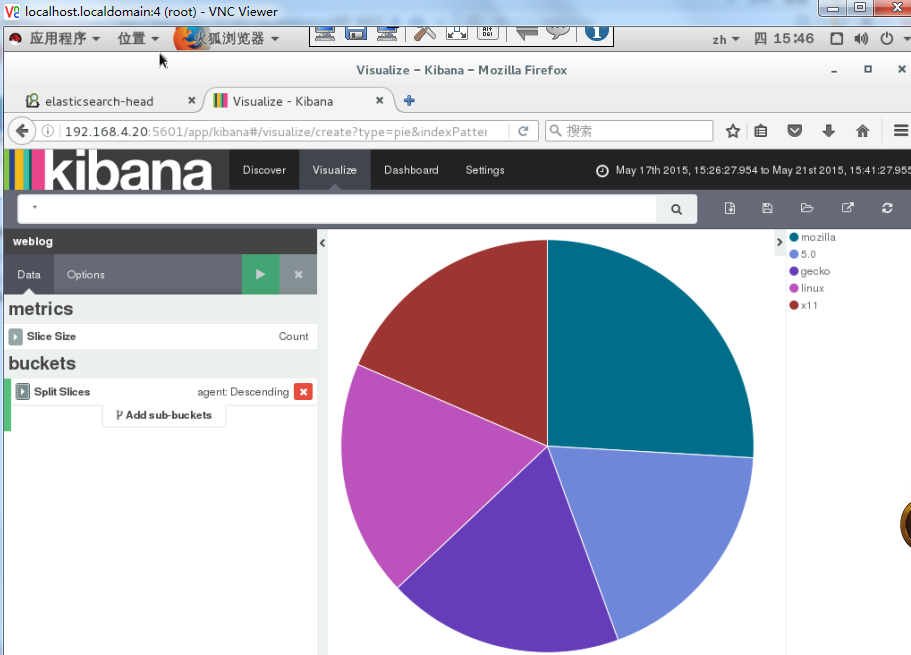


#修改分析时间





#展示图形



##配置日志推送

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

beats{

port => 5044

codec => "json"

}

file{

start\_position => "beginning"

sincedb\_path => "/dev/null"

path => ["/tmp/alog" ]

type => 'filelog'

codec => "json"

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

}

#信息输出模块

output{

if [type] == "filelog"{

elasticsearch {

hosts => ["192.168.4.21:9200", "192.168.4.22:9200"]

index => "weblog"

flush\_size => 2000

idle\_flush\_time => 10

}

}

}

[root@elk01 ~]# netstat -antpu

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 1/systemd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 816/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 919/master

tcp 0 0 0.0.0.0:5601 0.0.0.0:\* LISTEN 3841/node

tcp 0 0 192.168.4.20:59678 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59654 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59552 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59586 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59666 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59616 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59574 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59582 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59590 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59626 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59576 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59534 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59556 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59646 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59658 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59670 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59664 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59572 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59624 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59692 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59564 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59640 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59686 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59694 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59528 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59562 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59580 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59604 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59622 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59684 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59652 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:22 192.168.4.254:43640 ESTABLISHED 3905/sshd: root@pts

tcp 0 0 192.168.4.20:59560 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59602 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59690 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59674 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59546 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59636 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59598 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59536 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59632 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59554 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59584 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59608 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59544 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:22 192.168.4.254:43638 ESTABLISHED 3867/sshd: root@pts

tcp 0 0 192.168.4.20:59532 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59588 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59612 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59540 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59662 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59596 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59644 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59600 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59610 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59630 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59618 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59614 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59594 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59676 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59680 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59628 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59570 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59638 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59592 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59550 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59566 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59668 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59538 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59682 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59648 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59620 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59660 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59568 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:22 192.168.4.254:43412 ESTABLISHED 1027/sshd: root@pts

tcp 0 0 192.168.4.20:59542 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59650 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59688 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59558 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59530 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59606 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59578 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59656 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59642 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59672 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59634 192.168.4.21:9200 TIME\_WAIT -

tcp 0 0 192.168.4.20:59548 192.168.4.21:9200 TIME\_WAIT -

tcp6 0 0 :::111 :::\* LISTEN 1/systemd

tcp6 0 0 :::5044 :::\* LISTEN 4311/java

tcp6 0 0 :::22 :::\* LISTEN 816/sshd

tcp6 0 0 :::8888 :::\* LISTEN 4311/java

tcp6 0 0 ::1:25 :::\* LISTEN 919/master

tcp6 0 0 192.168.4.20:514 :::\* LISTEN 4311/java

tcp6 0 0 192.168.4.20:59140 192.168.4.21:9200 ESTABLISHED 4311/java

tcp6 0 0 192.168.4.20:58570 192.168.4.22:9200 ESTABLISHED 4311/java

udp 0 0 127.0.0.1:323 0.0.0.0:\* 528/chronyd

udp6 0 0 :::9999 :::\* 4311/java

udp6 0 0 ::1:323 :::\* 528/chronyd

udp6 0 0 192.168.4.20:514 :::\* 4311/java

#确认监听5044端口

[root@elk01 ~]# cat /etc/logstash/logstash.conf

#接受信息模块

input{

beats{

port => 5044

codec => "json"

type => "testlog"

}

file{

start\_position => "beginning"

sincedb\_path => "/var/lib/logstash/sinedb-access"

path => ["/tmp/alog" ]

type => 'filelog'

codec => "json"

}

tcp{

host => "0.0.0.0"

port => 8888

type => "tcplog"

}

udp{

host => "0.0.0.0"

port => 9999

type => "udplog"

}

syslog{

host => "192.168.4.20"

port => 514

type => "syslog"

}

}

#信息处理模块

filter{

}

#信息输出模块

output{

if [type] == "filelog"{

elasticsearch {

hosts => ["192.168.4.21:9200", "192.168.4.22:9200"]

index => "weblog"

flush\_size => 2000

idle\_flush\_time => 10

}

}

stdout{ codec => "rubydebug" }

}

[root@elk01 ~]# > /tmp/alog

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

[root@elk01 ~]# netstat -anptu | grep :5044

tcp6 0 0 :::5044 :::\* LISTEN 1048/java

[root@elk01 ~]# yum list | grep filebeat

filebeat.x86\_64 1.2.3-1 ELK

[root@elk01 ~]# yum -y install filebeat

已加载插件：langpacks, product-id, search-disabled-repos, subscription-manager

This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.

ELK | 2.9 kB 00:00

development | 4.1 kB 00:00

正在解决依赖关系

--> 正在检查事务

---> 软件包 filebeat.x86\_64.0.1.2.3-1 将被 安装

--> 解决依赖关系完成

依赖关系解决

===========================================================================

Package 架构 版本 源 大小

===========================================================================

正在安装:

filebeat x86\_64 1.2.3-1 ELK 3.9 M

事务概要

===========================================================================

安装 1 软件包

总下载量：3.9 M

安装大小：13 M

Downloading packages:

filebeat-1.2.3-x86\_64.rpm | 3.9 MB 00:00

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

正在安装 : filebeat-1.2.3-1.x86\_64 1/1

验证中 : filebeat-1.2.3-1.x86\_64 1/1

已安装:

filebeat.x86\_64 0:1.2.3-1

完毕！

#filebeat采用yaml格式

[root@elk01 ~]# systemctl start elasticsearch.service

[root@elk01 ~]# systemctl enable elasticsearch.service

Created symlink from /etc/systemd/system/multi-user.target.wants/elasticsearch.service to /usr/lib/systemd/system/elasticsearch.service.

[root@elk01 ~]# cat /etc/filebeat/filebeat.yml | grep -Pv "^(\s\*#|$)"

filebeat:

prospectors:

-

paths:

- /tmp/blog

input\_type: testlog

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

output:

logstash:

hosts: ["192.168.4.20:5044"]

shipper:

logging:

files:

rotateeverybytes: 10485760 # = 10MB

[root@elk01 ~]# touch /tmp/blog

[root@elk01 ~]# systemctl start filebeat.service ; systemctl enable filebeat.service

Created symlink from /etc/systemd/system/multi-user.target.wants/filebeat.service to /usr/lib/systemd/system/filebeat.service.

[root@elk01 ~]# head -n 5 /root/weblog >> /tmp/blog #测试日志

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

UDP listener died {:exception=>#<IOError: closed stream>, :backtrace=>["org/jruby/RubyIO.java:3682:in `select'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:77:in `udp\_listener'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:50:in `run'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:342:in `inputworker'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:336:in `start\_input'"], :level=>:warn}

^CSIGINT received. Terminating immediately.. {:level=>:fatal}

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# vim /etc/logstash/logstash.conf

[root@elk01 ~]# vim /etc/logstash/logstash.conf

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

UDP listener died {:exception=>#<IOError: closed stream>, :backtrace=>["org/jruby/RubyIO.java:3682:in `select'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:77:in `udp\_listener'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:50:in `run'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:342:in `inputworker'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:336:in `start\_input'"], :level=>:warn}

Pipeline main has been shutdown

^C^C[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

UDP listener died {:exception=>#<IOError: closed stream>, :backtrace=>["org/jruby/RubyIO.java:3682:in `select'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:77:in `udp\_listener'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:50:in `run'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:342:in `inputworker'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:336:in `start\_input'"], :level=>:warn}

^CSIGINT received. Terminating immediately.. {:level=>:fatal}

^C^C^C[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

UDP listener died {:exception=>#<IOError: closed stream>, :backtrace=>["org/jruby/RubyIO.java:3682:in `select'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:77:in `udp\_listener'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:50:in `run'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:342:in `inputworker'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:336:in `start\_input'"], :level=>:warn}

^CSIGINT received. Terminating immediately.. {:level=>:fatal}

^C^C[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# ^C

[root@elk01 ~]# vim /etc/logstash/logstash.conf

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"@timestamp" => "2018-01-25T16:27:48.521Z",

"ip" => "134.161.64.242",

"extension" => "css",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 62.64858333,

"lon" => -160.1898889

},

"src" => "US",

"dest" => "CS",

"srcdest" => "US:CS"

},

"@tags" => [

[0] "warning",

[1] "info"

],

"utc\_time" => "2015-05-20T14:46:52.269Z",

"referer" => "http://www.slate.com/error/andr-kuipers",

"agent" => "Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",

"clientip" => "134.161.64.242",

"bytes" => 4116,

"host" => "cdn.theacademyofperformingartsandscience.org",

"request" => "/styles/ad-blocker.css",

"url" => "https://cdn.theacademyofperformingartsandscience.org/styles/ad-blocker.css",

"@message" => "134.161.64.242 - - [2015-05-20T14:46:52.269Z] \"GET /styles/ad-blocker.css HTTP/1.1\" 200 4116 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>albert-sacco</h5>",

[1] "http://www.slate.com/success/carlos-i-noriega"

],

"links" => [

[0] "maksim-surayev@twitter.com",

[1] "http://twitter.com/login/liu-wang",

[2] "www.www.slate.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"og:type" => "article",

"og:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"og:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"og:url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"article:published\_time" => "2008-03-03T15:45:41-08:00",

"article:modified\_time" => "2014-11-27T10:00:32-08:00",

"article:section" => "Music",

"og:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"og:image:height" => "723",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"twitter:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"twitter:site" => "@laweekly"

},

[1] {

"url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"og:type" => "article",

"og:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"og:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"og:url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"article:published\_time" => "2008-03-06T11:00:00-08:00",

"article:modified\_time" => "2014-11-27T06:47:46-08:00",

"article:section" => "Music",

"article:tag" => "Donald Judd",

"og:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"og:image:height" => "468",

"og:image:width" => "535",

"og:site\_name" => "LA Weekly",

"twitter:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"twitter:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"twitter:site" => "@laweekly"

},

[2] {

"url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"og:type" => "article",

"og:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"og:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"og:url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"article:published\_time" => "2008-01-22T09:07:07-08:00",

"article:modified\_time" => "2014-11-27T06:47:35-08:00",

"article:section" => "Music",

"article:tag" => "Jonny Bell",

"og:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"og:image:height" => "359",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"twitter:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"twitter:site" => "@laweekly"

},

[3] {

"url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"og:type" => "article",

"og:title" => "Black Rock City Hit Parade",

"og:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"og:url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"article:published\_time" => "2007-08-31T13:41:39-07:00",

"article:modified\_time" => "2014-11-27T09:41:10-08:00",

"article:section" => "Music",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Black Rock City Hit Parade",

"twitter:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

},

[4] {

"url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"og:type" => "article",

"og:title" => "Calvin Harris, Henry Fonda, 4/23",

"og:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"og:url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"article:published\_time" => "2008-04-24T08:45:07-07:00",

"article:modified\_time" => "2014-11-27T08:57:00-08:00",

"article:section" => "Music",

"article:tag" => "Timothy Norris",

"og:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"og:image:height" => "319",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Calvin Harris, Henry Fonda, 4/23",

"twitter:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "win 8",

"ram" => 4294967296

},

"@version" => "1",

"type" => "log",

"input\_type" => "log",

"fields" => nil,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"source" => "/tmp/blog",

"offset" => 24957,

"count" => 1,

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

^CSIGINT received. Shutting down the agent. {:level=>:warn}

stopping pipeline {:id=>"main"}

UDP listener died {:exception=>#<IOError: closed stream>, :backtrace=>["org/jruby/RubyIO.java:3682:in `select'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:77:in `udp\_listener'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-udp-2.0.5/lib/logstash/inputs/udp.rb:50:in `run'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:342:in `inputworker'", "/opt/logstash/vendor/bundle/jruby/1.9/gems/logstash-core-2.3.4-java/lib/logstash/pipeline.rb:336:in `start\_input'"], :level=>:warn}

^CSIGINT received. Terminating immediately.. {:level=>:fatal}

[root@elk01 ~]# ^C

[root@elk01 ~]# logstash -f /etc/logstash/logstash.conf

Settings: Default pipeline workers: 1

Pipeline main started

{

"@timestamp" => "2018-01-25T16:29:33.666Z",

"ip" => "185.124.182.126",

"extension" => "gif",

"response" => "404",

"geo" => {

"coordinates" => {

"lat" => 36.518375,

"lon" => -86.05828083

},

"src" => "PH",

"dest" => "MM",

"srcdest" => "PH:MM"

},

"@tags" => [

[0] "success",

[1] "info"

],

"utc\_time" => "2015-05-18T09:03:25.877Z",

"referer" => "http://twitter.com/error/william-shepherd",

"agent" => "Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",

"clientip" => "185.124.182.126",

"bytes" => 804,

"host" => "motion-media.theacademyofperformingartsandscience.org",

"request" => "/canhaz/gemini-7.gif",

"url" => "https://motion-media.theacademyofperformingartsandscience.org/canhaz/gemini-7.gif",

"@message" => "185.124.182.126 - - [2015-05-18T09:03:25.877Z] \"GET /canhaz/gemini-7.gif HTTP/1.1\" 404 804 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>f-i-j-nl-ng</h5>",

[1] "http://facebook.com/success/lodewijk-van-den-berg"

],

"links" => [

[0] "daniel-tani@facebook.com",

[1] "http://nytimes.com/security/kathryn-sullivan",

[2] "www.nytimes.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/news/cbs-crew-rat-fink-2368032",

"og:type" => "article",

"og:title" => "CBS Crew Rat Fink",

"og:description" => "Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...",

"og:url" => "http://www.laweekly.com/news/cbs-crew-rat-fink-2368032",

"article:published\_time" => "2008-01-14T08:05:26-08:00",

"article:modified\_time" => "2014-10-28T14:59:52-07:00",

"article:section" => "News",

"article:tag" => "Mark Mauer",

"og:image" => "http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg",

"og:image:height" => "360",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "CBS Crew Rat Fink",

"twitter:description" => "Near a couple of auto body shops (and a sharp new Space Invader mosaic that we&#039;ll post soon) near Temple and Westmoreland is a CBS wall with a nice Rat ...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/cbs-crew-rat-fink/u/original/2430299/img\_2049.jpg",

"twitter:site" => "@laweekly"

},

[1] {

"url" => "http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043",

"og:type" => "article",

"og:title" => "Push and Retna in Koreatown",

"og:description" => "Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...",

"og:url" => "http://www.laweekly.com/news/push-and-retna-in-koreatown-2368043",

"article:published\_time" => "2008-01-29T07:28:32-08:00",

"article:modified\_time" => "2014-10-28T14:59:54-07:00",

"article:section" => "News",

"article:tag" => "Shelley Leopold",

"og:image" => "http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg",

"og:image:height" => "360",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Push and Retna in Koreatown",

"twitter:description" => "Yeah, I originally had this posted this morning as Push &amp; Ayer - Sorry. It looked like a Retna piece, but I saw the Ayer in there and thought that must ...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/push-and-retna-in-koreatown/u/original/2430376/img\_3671.jpg",

"twitter:site" => "@laweekly"

},

[2] {

"url" => "http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012",

"og:type" => "article",

"og:title" => "Asylm, Ruets, PDB on Santa Monica",

"og:description" => "Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...",

"og:url" => "http://www.laweekly.com/news/asylm-ruets-pdb-on-santa-monica-2368012",

"article:published\_time" => "2008-04-22T15:11:15-07:00",

"article:modified\_time" => "2014-10-28T14:59:48-07:00",

"article:section" => "News",

"article:tag" => "Culture and Lifestyle",

"og:image" => "http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg",

"og:image:height" => "360",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Asylm, Ruets, PDB on Santa Monica",

"twitter:description" => "Not a new piece, but a well-hidden gem a little south of Santa Monica Blvd. in an alley off of Heliotrope or Edgemont. I&#039;ve been sitting on this for a w...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/asylm-ruets-pdb-on-santa-monica/u/original/2430137/img\_5027.jpg",

"twitter:site" => "@laweekly"

},

[3] {

"url" => "http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867",

"og:type" => "article",

"og:title" => "Laurence Tribe Tangles with CBS and L.A. City Hall",

"og:description" => "The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...",

"og:url" => "http://www.laweekly.com/news/laurence-tribe-tangles-with-cbs-and-la-city-hall-2396867",

"article:published\_time" => "2008-06-04T14:16:10-07:00",

"article:modified\_time" => "2014-11-26T14:43:59-08:00",

"article:section" => "News",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Laurence Tribe Tangles with CBS and L.A. City Hall",

"twitter:description" => "The United States Court of Appeals for the Ninth Circuit&rsquo;s Courtroom 3 - a miniature auditorium with comfortable, smoked salmon-colored seats - wa...",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "win xp",

"ram" => 3221225472

},

"@version" => "1",

"source" => "/tmp/blog",

"input\_type" => "log",

"count" => 1,

"fields" => nil,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"offset" => 0,

"type" => "log",

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

{

"@timestamp" => "2018-01-25T16:29:33.674Z",

"ip" => "79.1.14.87",

"extension" => "gif",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 35.16531472,

"lon" => -107.9006142

},

"src" => "GN",

"dest" => "US",

"srcdest" => "GN:US"

},

"@tags" => [

[0] "success",

[1] "info"

],

"utc\_time" => "2015-05-18T12:28:25.013Z",

"referer" => "http://www.slate.com/warning/b-alvin-drew",

"agent" => "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24",

"clientip" => "79.1.14.87",

"bytes" => 774,

"host" => "motion-media.theacademyofperformingartsandscience.org",

"request" => "/canhaz/james-mcdivitt.gif",

"url" => "https://motion-media.theacademyofperformingartsandscience.org/canhaz/james-mcdivitt.gif",

"@message" => "79.1.14.87 - - [2015-05-18T12:28:25.013Z] \"GET /canhaz/james-mcdivitt.gif HTTP/1.1\" 200 774 \"-\" \"Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>charles-bolden</h5>",

[1] "http://www.slate.com/success/barry-wilmore"

],

"links" => [

[0] "george-nelson@twitter.com",

[1] "http://facebook.com/info/anatoly-solovyev",

[2] "www.www.slate.com"

],

"relatedContent" => [],

"machine" => {

"os" => "osx",

"ram" => 8589934592

},

"@version" => "1",

"type" => "log",

"input\_type" => "log",

"count" => 1,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"source" => "/tmp/blog",

"offset" => 5477,

"fields" => nil,

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

{

"@timestamp" => "2018-01-25T16:29:33.674Z",

"ip" => "178.209.1.7",

"extension" => "php",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 36.38025,

"lon" => -88.98547778

},

"src" => "US",

"dest" => "ET",

"srcdest" => "US:ET"

},

"@tags" => [

[0] "success",

[1] "security"

],

"utc\_time" => "2015-05-18T17:44:34.357Z",

"referer" => "http://facebook.com/success/voskhod-1",

"agent" => "Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24",

"clientip" => "178.209.1.7",

"bytes" => 7417,

"host" => "theacademyofperformingartsandscience.org",

"request" => "/people/type:astronauts/name:john-phillips/profile",

"memory" => 296680,

"phpmemory" => 296680,

"url" => "https://theacademyofperformingartsandscience.org/people/type:astronauts/name:john-phillips/profile",

"@message" => "178.209.1.7 - - [2015-05-18T17:44:34.357Z] \"GET /people/type:astronauts/name:john-phillips/profile HTTP/1.1\" 200 7417 \"-\" \"Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>scott-parazynski</h5>",

[1] "http://twitter.com/success/carl-walz"

],

"links" => [

[0] "lee-morin@www.slate.com",

[1] "http://facebook.com/info/oleg-makarov",

[2] "www.twitter.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/news/entropy-at-the-french-cottage-hollywood-2368119",

"og:type" => "article",

"og:title" => "Entropy at the French Cottage, Hollywood",

"og:description" => "The French Cottage hotel stood a few feet away from Sunset and Highland, near a stretch of old hotels and motels which are vanishing as steadily and unn...",

"og:url" => "http://www.laweekly.com/news/entropy-at-the-french-cottage-hollywood-2368119",

"article:published\_time" => "2007-08-09T08:48:14-07:00",

"article:modified\_time" => "2014-10-28T15:00:07-07:00",

"article:section" => "News",

"og:image" => "http://images1.laweekly.com/imager/entropy-at-the-french-cottage-hollywood/u/original/2430875/img\_1444.jpg",

"og:image:height" => "480",

"og:image:width" => "640",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Entropy at the French Cottage, Hollywood",

"twitter:description" => "The French Cottage hotel stood a few feet away from Sunset and Highland, near a stretch of old hotels and motels which are vanishing as steadily and unn...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/entropy-at-the-french-cottage-hollywood/u/original/2430875/img\_1444.jpg",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "win 8",

"ram" => 15032385536

},

"@version" => "1",

"count" => 1,

"fields" => nil,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"source" => "/tmp/blog",

"offset" => 6742,

"input\_type" => "log",

"type" => "log",

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

{

"@timestamp" => "2018-01-25T16:29:33.676Z",

"ip" => "118.140.92.127",

"extension" => "jpg",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 35.222595,

"lon" => -83.41904389

},

"src" => "BD",

"dest" => "PK",

"srcdest" => "BD:PK"

},

"@tags" => [

[0] "error",

[1] "info"

],

"utc\_time" => "2015-05-18T13:04:18.120Z",

"referer" => "http://www.slate.com/success/wendy-lawrence",

"agent" => "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)",

"clientip" => "118.140.92.127",

"bytes" => 9860,

"host" => "media-for-the-masses.theacademyofperformingartsandscience.org",

"request" => "/uploads/jeremy-hansen.jpg",

"url" => "https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/jeremy-hansen.jpg",

"@message" => "118.140.92.127 - - [2015-05-18T13:04:18.120Z] \"GET /uploads/jeremy-hansen.jpg HTTP/1.1\" 200 9860 \"-\" \"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>mary-weber</h5>",

[1] "http://twitter.com/warning/ellen-s-baker"

],

"links" => [

[0] "g-david-low@www.slate.com",

[1] "http://www.slate.com/info/mario-runco-jr-",

[2] "www.www.slate.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/arts/rain-rain-go-away-charlize-theron-wants-to-play-2371781",

"og:type" => "article",

"og:title" => "Rain Rain Go Away Charlize Theron Wants To Play",

"og:description" => "LA Weekly is the definitive source of information for news, music, movies, restaurants, reviews, and events in Los Angeles.",

"og:url" => "http://www.laweekly.com/arts/rain-rain-go-away-charlize-theron-wants-to-play-2371781",

"article:published\_time" => "2005-10-18T08:10:44-07:00",

"article:modified\_time" => "2014-11-25T18:34:34-08:00",

"article:section" => "Arts",

"article:tag" => "Celebrity News",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Rain Rain Go Away Charlize Theron Wants To Play",

"twitter:description" => "LA Weekly is the definitive source of information for news, music, movies, restaurants, reviews, and events in Los Angeles.",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

},

[1] {

"url" => "http://www.laweekly.com/news/camera-eye-santa-monica-and-myra-2368130",

"og:type" => "article",

"og:title" => "Camera Eye - Santa Monica and Myra",

"og:description" => "All photos by Mark Mauer...",

"og:url" => "http://www.laweekly.com/news/camera-eye-santa-monica-and-myra-2368130",

"article:published\_time" => "2007-08-12T22:41:49-07:00",

"article:modified\_time" => "2014-10-28T15:00:10-07:00",

"article:section" => "News",

"article:tag" => "Mark Mauer",

"og:image" => "http://images1.laweekly.com/imager/camera-eye-santa-monica-and-myra/u/original/2430949/1632.jpg",

"og:image:height" => "640",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Camera Eye - Santa Monica and Myra",

"twitter:description" => "All photos by Mark Mauer...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/camera-eye-santa-monica-and-myra/u/original/2430949/1632.jpg",

"twitter:site" => "@laweekly"

},

[2] {

"url" => "http://www.laweekly.com/news/rime-show-at-ghettogloss-2368009",

"og:type" => "article",

"og:title" => "Rime Show at Ghettogloss",

"og:description" => "Seventh Letter crew member RIME, aka Jersey Joe, will be showing new work at Ghettogloss this Friday, March 7. The show will run for a couple of weeks, ...",

"og:url" => "http://www.laweekly.com/news/rime-show-at-ghettogloss-2368009",

"article:published\_time" => "2008-03-03T14:05:13-08:00",

"article:modified\_time" => "2014-10-28T14:59:48-07:00",

"article:section" => "News",

"article:tag" => "Business",

"og:image" => "http://images1.laweekly.com/imager/rime-show-at-ghettogloss/u/original/2430136/gg08\_flyer\_l.jpg",

"og:image:height" => "539",

"og:image:width" => "792",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Rime Show at Ghettogloss",

"twitter:description" => "Seventh Letter crew member RIME, aka Jersey Joe, will be showing new work at Ghettogloss this Friday, March 7. The show will run for a couple of weeks, ...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/rime-show-at-ghettogloss/u/original/2430136/gg08\_flyer\_l.jpg",

"twitter:site" => "@laweekly"

},

[3] {

"url" => "http://www.laweekly.com/music/greetings-from-the-first-annual-marfa-film-festival-2404240",

"og:type" => "article",

"og:title" => "Greetings from the first annual Marfa Film Festival",

"og:description" => "I got on a bus in Los Feliz yesterday at about 1 p.m. headed for Marfa, Texas, to attend the first annual Marfa Film Festival. If you&#039;ve been to the mov...",

"og:url" => "http://www.laweekly.com/music/greetings-from-the-first-annual-marfa-film-festival-2404240",

"article:published\_time" => "2008-05-02T05:38:40-07:00",

"article:modified\_time" => "2014-11-27T07:22:29-08:00",

"article:section" => "Music",

"og:image" => "http://IMAGES1.laweekly.com/imager/greetings-from-the-first-annual-marfa-film/u/original/2466493/marfateaparty.jpg",

"og:image:height" => "688",

"og:image:width" => "550",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Greetings from the first annual Marfa Film Festival",

"twitter:description" => "I got on a bus in Los Feliz yesterday at about 1 p.m. headed for Marfa, Texas, to attend the first annual Marfa Film Festival. If you&#039;ve been to the mov...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/greetings-from-the-first-annual-marfa-film/u/original/2466493/marfateaparty.jpg",

"twitter:site" => "@laweekly"

},

[4] {

"url" => "http://www.laweekly.com/arts/the-fug-girls-on-rock-and-republic-in-new-york-72-separate-skanky-looks-2372847",

"og:type" => "article",

"og:title" => "The Fug Girls on Rock &amp; Republic in New York: &quot;72 separate, skanky looks!&quot;",

"og:description" => "LA Weekly is the definitive source of information for news, music, movies, restaurants, reviews, and events in Los Angeles.",

"og:url" => "http://www.laweekly.com/arts/the-fug-girls-on-rock-and-republic-in-new-york-72-separate-skanky-looks-2372847",

"article:published\_time" => "2007-02-04T10:02:17-08:00",

"article:modified\_time" => "2014-11-25T19:27:51-08:00",

"article:section" => "Arts",

"og:site\_name" => "LA Weekly",

"twitter:title" => "The Fug Girls on Rock &amp; Republic in New York: &quot;72 separate, skanky looks!&quot;",

"twitter:description" => "LA Weekly is the definitive source of information for news, music, movies, restaurants, reviews, and events in Los Angeles.",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "osx",

"ram" => 20401094656

},

"@version" => "1",

"count" => 1,

"fields" => nil,

"source" => "/tmp/blog",

"offset" => 9244,

"type" => "log",

"input\_type" => "log",

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

{

"@timestamp" => "2018-01-25T16:29:33.676Z",

"ip" => "235.154.34.221",

"extension" => "jpg",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 46.94100778,

"lon" => -98.01762611

},

"src" => "BY",

"dest" => "KE",

"srcdest" => "BY:KE"

},

"@tags" => [

[0] "success",

[1] "login"

],

"utc\_time" => "2015-05-18T11:37:40.653Z",

"referer" => "http://www.slate.com/success/edward-lu",

"agent" => "Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",

"clientip" => "235.154.34.221",

"bytes" => 4191,

"host" => "media-for-the-masses.theacademyofperformingartsandscience.org",

"request" => "/uploads/eugene-trinh.jpg",

"url" => "https://media-for-the-masses.theacademyofperformingartsandscience.org/uploads/eugene-trinh.jpg",

"@message" => "235.154.34.221 - - [2015-05-18T11:37:40.653Z] \"GET /uploads/eugene-trinh.jpg HTTP/1.1\" 200 4191 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>susan-still-kilrain</h5>",

[1] "http://www.slate.com/success/timothy-l-kopra"

],

"links" => [

[0] "stephen-oswald@nytimes.com",

[1] "http://www.slate.com/info/sigmund-j-hn",

[2] "www.twitter.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/news/once-more-in-the-river-2368108",

"og:type" => "article",

"og:title" => "Once more in the River",

"og:description" => "All photos by Mark Mauer. More after the jump...",

"og:url" => "http://www.laweekly.com/news/once-more-in-the-river-2368108",

"article:published\_time" => "2007-10-15T10:46:29-07:00",

"article:modified\_time" => "2014-10-28T15:00:05-07:00",

"article:section" => "News",

"og:image" => "http://IMAGES1.laweekly.com/imager/once-more-in-the-river/u/original/2430775/img\_2536.jpg",

"og:image:height" => "640",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Once more in the River",

"twitter:description" => "All photos by Mark Mauer. More after the jump...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/once-more-in-the-river/u/original/2430775/img\_2536.jpg",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"ram" => 4294967296

},

"@version" => "1",

"input\_type" => "log",

"fields" => nil,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"source" => "/tmp/blog",

"offset" => 15545,

"type" => "log",

"count" => 1,

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

#监控端显示数据

[root@elk01 ~]# tail -n 1 /root/weblog >> /tmp/blog

{

"@timestamp" => "2018-01-25T16:31:08.686Z",

"ip" => "134.161.64.242",

"extension" => "css",

"response" => "200",

"geo" => {

"coordinates" => {

"lat" => 62.64858333,

"lon" => -160.1898889

},

"src" => "US",

"dest" => "CS",

"srcdest" => "US:CS"

},

"@tags" => [

[0] "warning",

[1] "info"

],

"utc\_time" => "2015-05-20T14:46:52.269Z",

"referer" => "http://www.slate.com/error/andr-kuipers",

"agent" => "Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1",

"clientip" => "134.161.64.242",

"bytes" => 4116,

"host" => "cdn.theacademyofperformingartsandscience.org",

"request" => "/styles/ad-blocker.css",

"url" => "https://cdn.theacademyofperformingartsandscience.org/styles/ad-blocker.css",

"@message" => "134.161.64.242 - - [2015-05-20T14:46:52.269Z] \"GET /styles/ad-blocker.css HTTP/1.1\" 200 4116 \"-\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:6.0a1) Gecko/20110421 Firefox/6.0a1\"",

"spaces" => "this is a thing with lots of spaces wwwwoooooo",

"xss" => "<script>console.log(\"xss\")</script>",

"headings" => [

[0] "<h3>albert-sacco</h5>",

[1] "http://www.slate.com/success/carlos-i-noriega"

],

"links" => [

[0] "maksim-surayev@twitter.com",

[1] "http://twitter.com/login/liu-wang",

[2] "www.www.slate.com"

],

"relatedContent" => [

[0] {

"url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"og:type" => "article",

"og:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"og:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"og:url" => "http://www.laweekly.com/music/grizzly-bear-and-the-los-angeles-philharmonic-at-walt-disney-concert-hall-march-1-2411954",

"article:published\_time" => "2008-03-03T15:45:41-08:00",

"article:modified\_time" => "2014-11-27T10:00:32-08:00",

"article:section" => "Music",

"og:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"og:image:height" => "723",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Grizzly Bear and the Los Angeles Philharmonic at Walt Disney Concert Hall, March 1",

"twitter:description" => "Grizzly Bear and the Los Angeles Philharmonic Walt Disney Concert Hall Saturday, March 1 photos by Timothy Norris You knew Saturday night was turning ma...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/grizzly-bear-and-the-los-angeles-philharmo/u/original/2474805/grizzlybeartn034.jpg",

"twitter:site" => "@laweekly"

},

[1] {

"url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"og:type" => "article",

"og:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"og:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"og:url" => "http://www.laweekly.com/music/cold-desolate-places-phil-elverum-aka-the-microphones-aka-mt-eerie-interviewed-part-1-of-4-2410936",

"article:published\_time" => "2008-03-06T11:00:00-08:00",

"article:modified\_time" => "2014-11-27T06:47:46-08:00",

"article:section" => "Music",

"article:tag" => "Donald Judd",

"og:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"og:image:height" => "468",

"og:image:width" => "535",

"og:site\_name" => "LA Weekly",

"twitter:title" => "&ldquo;Cold Desolate Places&rdquo;: Phil Elverum (aka The Microphones aka Mt. Eerie) Interviewed: Part 1 of 4",

"twitter:description" => "Phil Elverum: &quot;It&#039;s so weird here right now. It&#039;s snowing but the sky is blue and it&#039;s not really that cold. I don&#039;t know where the flakes are coming fr...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/andldquocold-desolate-placesandrdquo-phil-e/u/original/2473683/080306\_teenagekicks\_elverumlake.jpg",

"twitter:site" => "@laweekly"

},

[2] {

"url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"og:type" => "article",

"og:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"og:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"og:url" => "http://www.laweekly.com/music/crystal-antlers-at-high-voltage-party-safari-sams-1-21-08-2410738",

"article:published\_time" => "2008-01-22T09:07:07-08:00",

"article:modified\_time" => "2014-11-27T06:47:35-08:00",

"article:section" => "Music",

"article:tag" => "Jonny Bell",

"og:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"og:image:height" => "359",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Crystal Antlers at High Voltage Party, Safari Sam&#039;s, 1/21/08",

"twitter:description" => "Crystal Antlers Safari Sam&#039;s, Jan. 21, 2008 The sparkling reputation of Long Beach&rsquo;s Crystal Antlers drew me out to the High Voltage Magazine part...",

"twitter:card" => "summary",

"twitter:image" => "http://images1.laweekly.com/imager/crystal-antlers-at-high-voltage-party-saf/u/original/2473410/img\_2120s.jpg",

"twitter:site" => "@laweekly"

},

[3] {

"url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"og:type" => "article",

"og:title" => "Black Rock City Hit Parade",

"og:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"og:url" => "http://www.laweekly.com/music/black-rock-city-hit-parade-2409397",

"article:published\_time" => "2007-08-31T13:41:39-07:00",

"article:modified\_time" => "2014-11-27T09:41:10-08:00",

"article:section" => "Music",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Black Rock City Hit Parade",

"twitter:description" => "By Randall Roberts Top Songs (that aren&rsquo;t trance or prog house) heard last night kicking out of any of the hundreds of rolling sound systems (or s...",

"twitter:card" => "summary",

"twitter:site" => "@laweekly"

},

[4] {

"url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"og:type" => "article",

"og:title" => "Calvin Harris, Henry Fonda, 4/23",

"og:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"og:url" => "http://www.laweekly.com/music/calvin-harris-henry-fonda-4-23-2403568",

"article:published\_time" => "2008-04-24T08:45:07-07:00",

"article:modified\_time" => "2014-11-27T08:57:00-08:00",

"article:section" => "Music",

"article:tag" => "Timothy Norris",

"og:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"og:image:height" => "319",

"og:image:width" => "480",

"og:site\_name" => "LA Weekly",

"twitter:title" => "Calvin Harris, Henry Fonda, 4/23",

"twitter:description" => "Photos from the Calvin Harris show, Wednesday night, at the Henry Fonda Theater by Timothy Norris More after the jump. All photos by Timothy Norris...",

"twitter:card" => "summary",

"twitter:image" => "http://IMAGES1.laweekly.com/imager/calvin-harris-henry-fonda-4-23/u/original/2465849/calvinharristn013.jpg",

"twitter:site" => "@laweekly"

}

],

"machine" => {

"os" => "win 8",

"ram" => 4294967296

},

"@version" => "1",

"source" => "/tmp/blog",

"type" => "log",

"offset" => 17610,

"input\_type" => "log",

"count" => 1,

"fields" => nil,

"beat" => {

"hostname" => "elk01",

"name" => "elk01"

},

"tags" => [

[0] "beats\_input\_codec\_json\_applied"

]

}

##测试完成