ELK环境搭建

1. Virtualbox/Vagrant安装 4

1.1. Virtualbox安装 4

1.2. Vagrant安装 4

1.2.1. 简述 4

1.2.2. Vagrant box 4

1.2.3. 安装配置 5

1.2.4. 常用命令 6

2. ELK安装 6

2.1. CentOS7系统配置 6

2.1.1. 安装iptables 6

2.1.2. 安装ifconfig 6

2.1.3. 禁用IPV6 7

2.2. 安装Java并配置环境变量 7

2.3. 安装Elasticsearch 7

2.3.1. 导入elasticsearch公钥 7

2.3.2. 创建elasticsearch.repo 7

2.3.3. 使用yum install安装 8

2.3.4. 修改elasticsearch配置（修改主机ip） 8

2.3.5. 启动elasticsearch 8

2.3.6. 将elasticsearch添加到开机自启动 8

2.3.7. 访问elasticsearch rest服务 8

2.4. 安装Kibana 9

2.4.1. 创建kibana.repo 9

2.4.2. 使用yum install安装kibana 9

2.4.3. 修改kibana配置 9

2.4.4. 启动kibana并添加为开机自启动服务 9

2.5. 安装Nginx（此部分内容不是必须） 10

2.5.1. 安装nginx 10

2.5.2. 创建用户并设定密码 10

2.5.3. 修改/etc/nginx/nginx.conf 10

2.5.4. 创建/etc/nginx/conf.d/kibana.conf文件 11

2.5.5. 启动nginx并添加到开启自启动服务 11

2.6. 安装Logstash 11

2.6.1. 创建logstash.repo 12

2.6.2. 使用yum install安装logstash 12

2.6.3. 生成ssl证书 12

2.6.3.1. 根据ip生成 12

2.6.3.2. 根据域名生成 12

2.6.4. Logstash配置 13

2.6.4.1. Input 13

2.6.4.2. Filter 13

2.6.4.3. Output 14

2.6.5. 测试配置是否正确 14

2.6.6. 启动logstash并添加为开机自启动服务 14

2.6.7. 安装 Kibana Dashboards 14

2.7. 安装Filebeat 15

2.7.1. 导入elasticsearch公钥 15

2.7.2. 创建elastic-beats.repo 15

2.7.3. 安装filebeat 15

2.7.4. 配置Filebeat 15

2.7.4.1. 一个简单的配置 15

2.7.4.1.1. 使用elasticsearch作为输出 16

2.7.4.1.2. 使用logstash作为输出 16

2.7.5. load filebeat template 16

2.7.6. 启动filebeat并添加为系统开机自启动服务 17

2.7.7. 测试filebeat 17

2.7.8. Connect to Kibana 18

2.8. 安装topbeat 19

2.8.1. 导入elasticsearch公钥 19

2.8.2. 创建elastic-beats.repo 20

2.8.3. 安装topbeat 20

2.8.4. 配置Topbeat 20

2.8.5. load topbeat template 20

2.8.6. 启动topbeat并添加为系统开机自启动服务 21

2.8.7. 测试topbeat 21

2.8.8. Connect to Kibana 22

2.9. logstash扩展配置 23

2.9.1. Nginx日志配置 24

2.9.1.1. Logstash Patterns: Nginx 25

2.9.1.2. Logstash Filter: Nginx 25

2.9.1.3. 重启logstash 25

2.9.1.4. Filebeat Prospector: Nginx 25

2.9.1.5. 重启filebeat 26

2.9.1.6. kibana搜索效果图 26

2.9.2. Apache HTTP Web Server日志配置 26

2.9.2.1. Logstash Filter: Apache 26

2.9.2.2. 重启logstash 27

2.9.2.3. Filebeat Prospector: Apache 27

2.9.2.4. 重启filebeat 27

2.9.3. Tomcat日志配置 27

2.9.3.1. 定义Logstash Patterns: Tomcat 28

2.9.3.2. 定义Logstash Filter: Tomcat 28

2.9.3.3. 重启logstash 29

2.9.3.4. Filebeat Prospector: Tomcat 29

2.9.3.5. 重启filebeat 29

2.9.3.6. kibana搜索效果图 30

2.9.4. 最终配置 30

2.10. 使用Kibana查询分析日志 31

2.11. Elasticsearch插件安装 34

2.11.1. plugin命令介绍 35

2.11.2. 安装head插件 35

2.11.3. 安装bigdesk插件 37

2.11.4. 安装kopf插件 39

2.11.5. 插件列表 40

3. 参考资料 40

4. 使用Elasticsearch做全文检索 41

环境:

Vagrant 1.8.1

CentOS 7.2 192.168.0.228

Elasticsearch 2.3.2

logstash 2.2.4

Kibana 4.4.2

filebeat 1.2.2

topbeat 1.2.2

# Virtualbox/Vagrant安装

此部分内容不是必须，已有linux环境可跳过该步骤。

## Virtualbox安装

主页：<https://www.virtualbox.org/>

安装包：<http://download.virtualbox.org/virtualbox/5.0.20/VirtualBox-5.0.20-106931-Win.exe>

## Vagrant安装

主页：<https://www.vagrantup.com>

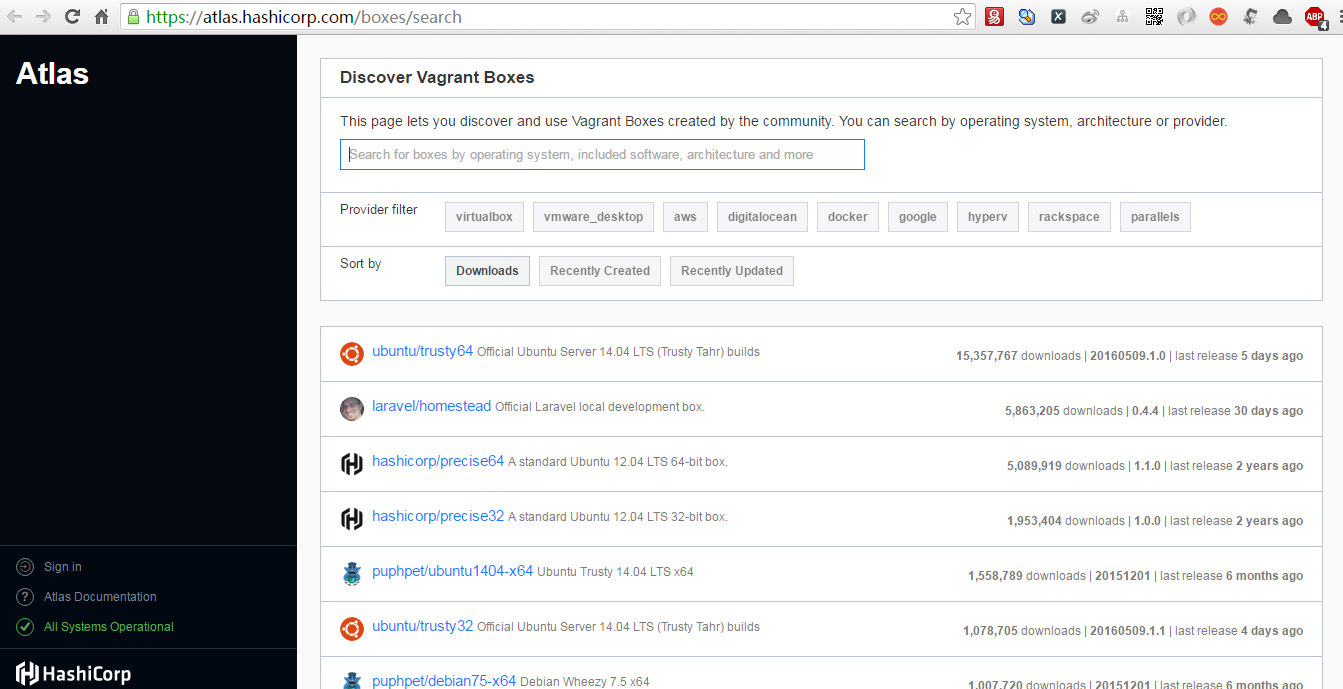
### 简述

Vagrant与Docker很像。Vagrant是一个基于Ruby的开源工具，用于创建和部署虚拟化开发环境。非常适合 php/python/ruby/java 这类语言开发 web 应用。它 使用Oracle的开源VirtualBox虚拟化系统。可以通过 Vagrant 封装一个 Linux 的开发环境，分发给团队成员。成员可以在自己喜欢的桌面系统（Mac/Windows/Linux）上开发程序，代码却能统一在封装好的环境里运行，非常霸气。

安装包：<https://releases.hashicorp.com/vagrant/1.8.1/vagrant_1.8.1.msi>下载下来直接安装。

### Vagrant box

Vagrant box镜像站点：<https://atlas.hashicorp.com/boxes/search>



### 安装配置

这里我们使用CentOS官方提供的vagrant box

<http://cloud.centos.org/centos/7/vagrant/x86_64/images/CentOS-7.box>

下载该box到本地，假若放在F:\目录下

添加本地box

vagrant box add CentOS/7 F:\CentOS-7.box # 添加本地box名称为CentOS/7

vagrant box list # 查看box列表

vagrant init CentOS/7 # 使用已添加的box创建虚拟机

vagrant up # 启动vagrant

最终会在目录下生成一个名为Vagrantfile的文件。

修改或编辑该文件内容如下

|  |
| --- |
| Vagrant.configure(2) do |config|  config.vm.box = "CentOS/7"  config.vm.network "public\_network", ip: "192.168.0.228"  config.vm.hostname = "c1"  config.vm.provider "virtualbox" do |vb|  vb.name = "c1"  vb.memory = "2048"  end  end |

注：其中config.vm.box表示使用哪个box，

config.vm.network 配置网络及ip，

config.vm.hostname设置主机名称，

config.vm.provider设置使用virtualbox当然你还可以使用vmware。

Vb.name设置主机名，

vb.memory设置内存大小。

使用vagrant up启动虚拟机。

### 常用命令

|  |
| --- |
| $ vagrant init # 初始化  $ vagrant up # 启动虚拟机  $ vagrant halt # 关闭虚拟机  $ vagrant reload # 重启虚拟机  $ vagrant ssh # SSH 至虚拟机  $ vagrant status # 查看虚拟机运行状态  $ vagrant destroy # 销毁当前虚拟机 |

关于vagrant的详细使用请参考<https://github.com/sxyx2008/DevArticles/issues/36>。此处不做赘述。

# ELK安装

## CentOS7系统配置

在开始安装elk之前，我们需要对CentOS7做一系列配置。CentOS7安装后默认没有安装ifconfig、iptables等命令。

### 安装iptables

|  |
| --- |
| $ systemctl stop firewalld  $ systemctl mask firewalld  $ yum install iptables-services  $ systemctl enable iptables  $ systemctl [stop|start|restart] iptables  $ service iptables save |

### 安装ifconfig

|  |
| --- |
| $ ip addr  $ ip link  $ ip -s link  $ yum provides ifconfig  $ yum whatprovides ifconfig  $ yum install net-tools  $ ifconfig -a |

### 禁用IPV6

方法一：

|  |
| --- |
| $ vi /etc/sysctl.conf  net.ipv6.conf.all.disable\_ipv6 = 1  net.ipv6.conf.eth1.disable\_ipv6 = 1  $ sysctl -p |

方法二：

|  |
| --- |
| $ vi /etc/sysctl.d/disableipv6.conf  net.ipv6.conf.all.disable\_ipv6 = 1  net.ipv6.conf.eth1.disable\_ipv6 = 1  $ reboot |

## 安装Java并配置环境变量

|  |
| --- |
| $ cd ~  $ wget --no-cookies --no-check-certificate --header "Cookie: gpw\_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie" "http://download.oracle.com/otn-pub/java/jdk/8u211-b02/jdk-8u211-linux-x64.rpm"  $ sudo yum -y localinstall jdk-8u73-linux-x64.rpm  $ sudo vim /etc/profile  export JAVA\_HOME=/usr/java/jdk1.8.0\_73  export CLASS\_PATH=.:$JAVA\_HOME/lib/dt.jar:$JAVA\_HOME/lib/tools.jar  export PATH=$JAVA\_HOME/bin:$PATH  $ source /etc/profile |

## 安装Elasticsearch

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

### 导入elasticsearch公钥

$ sudo rpm --import <http://packages.elastic.co/GPG-KEY-elasticsearch>

### 创建elasticsearch.repo

$ echo '[elasticsearch-2.x]

name=Elasticsearch repository for 2.x packages

baseurl=http://packages.elastic.co/elasticsearch/2.x/centos

gpgcheck=1

gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch

enabled=1

' | sudo tee /etc/yum.repos.d/elasticsearch.repo

### 使用yum install安装

$ sudo yum -y install elasticsearch

### 修改elasticsearch配置（修改主机ip）

$ sudo vim /etc/elasticsearch/elasticsearch.yml

network.host: 192.168.0.228

### 启动elasticsearch

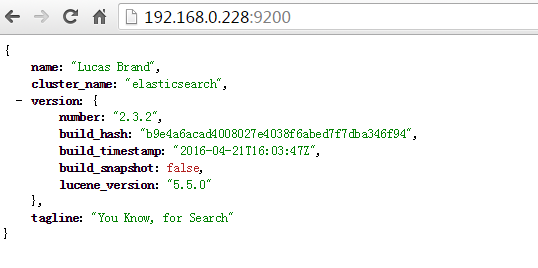
$ sudo systemctl start elasticsearch

### 将elasticsearch添加到开机自启动

$ sudo systemctl enable elasticsearch

### 访问elasticsearch rest服务

使用http://192.168.0.228:9200/出现如下内容表示elasticsearch安装成功。



注：

1. Elasticsearch默认http端口为9200，节点端口为9300
2. Elasticsearch rest服务访问不到则记得查看防火墙配置。
3. Elasticsearch默认安装到/usr/share/elasticsearch目录下
4. Elasticsearch配置文件默认在/etc/elasticsearch/目录下。可以使用rpm -qc命令查看。如下所示：

$ rpm -qc elasticsearch

/etc/elasticsearch/elasticsearch.yml

/etc/elasticsearch/logging.yml

/etc/init.d/elasticsearch

/etc/sysconfig/elasticsearch

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

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

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

## 安装Kibana

<https://www.elastic.co/guide/en/kibana/current/index.html>

### 创建kibana.repo

$ sudo vim /etc/yum.repos.d/kibana.repo

[kibana-4.4]

name=Kibana repository for 4.4.x packages

baseurl=http://packages.elastic.co/kibana/4.4/centos

gpgcheck=1

gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch

enabled=1

### 使用yum install安装kibana

$ sudo yum -y install kibana

注：

1. Kibana默认端口为5601
2. kibana默认安装在/opt/kibana目录下
3. Kibana配置文件路径为/opt/kibana/config/kibana.yml

$ rpm -qc kibana

/opt/kibana/config/kibana.yml

### 修改kibana配置

$ sudo vim /opt/kibana/config/kibana.yml

server.host: "192.168.0.228"

elasticsearch.url: "http://192.168.0.228:9200"

### 启动kibana并添加为开机自启动服务

$ sudo systemctl start kibana

$ sudo chkconfig kibana on

## 安装Nginx（此部分内容不是必须）

由于elasticsearch、kibana自身均没有提供访问权限安全问题，这里使用nginx代理来验证用户身份。

### 安装nginx

$ sudo yum -y install epel-release

$ sudo yum -y install nginx httpd-tools

### 创建用户并设定密码

$ sudo htpasswd -c /etc/nginx/htpasswd.users kibanaadmin #创建kibanaadmin用户

注：

这里创建的用户为kibanaadmin/kibanaadmin（用户密码均为kibanaadmin）

### 修改/etc/nginx/nginx.conf

$ sudo vim /etc/nginx/nginx.conf

|  |
| --- |
| user nginx;  worker\_processes auto;  error\_log /var/log/nginx/error.log;  pid /run/nginx.pid;  events {  worker\_connections 1024;  }  http {  log\_format main '$remote\_addr - $remote\_user [$time\_local] "$request" '  '$status $body\_bytes\_sent "$http\_referer" '  '"$http\_user\_agent" "$http\_x\_forwarded\_for"';  access\_log /var/log/nginx/access.log main;  sendfile on;  tcp\_nopush on;  tcp\_nodelay on;  keepalive\_timeout 65;  types\_hash\_max\_size 2048;  include /etc/nginx/mime.types;  default\_type application/octet-stream;  include /etc/nginx/conf.d/\*.conf;  } |

### 创建/etc/nginx/conf.d/kibana.conf文件

sudo vim /etc/nginx/conf.d/kibana.conf

|  |
| --- |
| server {  listen 80;  server\_name 192.168.0.228;  auth\_basic "Restricted Access";  auth\_basic\_user\_file /etc/nginx/htpasswd.users;  location / {  proxy\_pass http://192.168.0.228:5601;  proxy\_http\_version 1.1;  proxy\_set\_header Upgrade $http\_upgrade;  proxy\_set\_header Connection 'upgrade';  proxy\_set\_header Host $host;  proxy\_cache\_bypass $http\_upgrade;  }  } |

注：

1. 以上配置使用http basic认证用户身份。
2. 使用nginx反向代理到kibana所在服务器（http://192.168.0.228:5601）

为了使上述配置生效并能成功代理，需做如下操作

$ sudo setsebool -P httpd\_can\_network\_connect 1

至此，访问nginx时则会要求输入用户名密码（kibanaadmin/kibanaadmin）。输入正确后请求会请求代理到kibana

### 启动nginx并添加到开启自启动服务

$ sudo systemctl start nginx

$ sudo systemctl enable nginx

## 安装Logstash

<https://www.elastic.co/guide/en/logstash/current/index.html>

### 创建logstash.repo

$ sudo vim /etc/yum.repos.d/logstash.repo

[logstash-2.2]

name=logstash repository for 2.2 packages

baseurl=http://packages.elasticsearch.org/logstash/2.2/centos

gpgcheck=1

gpgkey=http://packages.elasticsearch.org/GPG-KEY-elasticsearch

enabled=1

### 使用yum install安装logstash

$ sudo yum -y install logstash

注：

1. logstash默认安装在/opt/logstash目录
2. Logstash默认配置文件目录rpm -qc logstash

/etc/init.d/logstash

/etc/logrotate.d/logstash

/etc/sysconfig/logstash

### 生成ssl证书

#### 根据ip生成

修改/etc/pki/tls/openssl.cnf文件，找到[ v3\_ca ]节点。修改subjectAltName为IP:ELK安装机器IP。

sudo vim /etc/pki/tls/openssl.cnf

内容如下：

[ v3\_ca ]

subjectAltName = IP: 192.168.0.228

切换到/etc/pki/tls目录，生成证书

$ cd /etc/pki/tls

$ sudo openssl req -config /etc/pki/tls/openssl.cnf -x509 -days 3650 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt

#### 根据域名生成

$ cd /etc/pki/tls

$ sudo openssl req -subj '/CN=www.elk.com/' -x509 -days 3650 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt

### Logstash配置

这里所有的配置均在/etc/logstash/conf.d目录下。

#### Input

创建一个beats input

$ sudo vim /etc/logstash/conf.d/02-beats-input.conf

input {

beats {

port => 5044

ssl => true

ssl\_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"

ssl\_key => "/etc/pki/tls/private/logstash-forwarder.key"

}

}

这里使用beats input，监听在5044端口上，使用之前生成的证书文件。

#### Filter

为syslog创建一个filter

$ sudo vim /etc/logstash/conf.d/10-syslog-filter.conf

filter {

if [type] == "syslog" {

grok {

match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{SYSLOGHOST:syslog\_hostname} %{DATA:syslog\_program}(?:\[%{POSINT:syslog\_pid}\])?: %{GREEDYDATA:syslog\_message}" }

add\_field => [ "received\_at", "%{@timestamp}" ]

add\_field => [ "received\_from", "%{host}" ]

}

syslog\_pri { }

date {

match => [ "syslog\_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]

}

}

}

#### Output

将beat输入输出到elasticsearch

$ sudo vim /etc/logstash/conf.d/30-elasticsearch-output.conf

output {

elasticsearch {

hosts => ["192.168.0.228:9200"]

sniffing => true

manage\_template => false

index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"

document\_type => "%{[@metadata][type]}"

}

}

### 测试配置是否正确

$ sudo service logstash configtest

如果显示Configuration OK则表示没有任何语法错误。

### 启动logstash并添加为开机自启动服务

$ sudo systemctl restart logstash

$ sudo chkconfig logstash on

### 安装 Kibana Dashboards

$ curl -L -O <http://download.elastic.co/beats/dashboards/beats-dashboards-1.2.2.zip>

$ unzip beats-dashboards-1.2.2.zip

$ cd beats-dashboards-1.2.2/

$ vim ./load.sh

ELASTICSEARCH=http://192.168.0.228:9200

$ ./load.sh

执行完后会创建如下index pattern

[packetbeat-]YYYY.MM.DD

[topbeat-]YYYY.MM.DD

[filebeat-]YYYY.MM.DD

[winlogbeat-]YYYY.MM.DD

使用kibana时，选择filebeat模式

## 安装Filebeat

<https://www.elastic.co/guide/en/beats/filebeat/1.2/index.html>

### 导入elasticsearch公钥

$ sudo rpm --import <http://packages.elastic.co/GPG-KEY-elasticsearch>

### 创建elastic-beats.repo

$ sudo vim /etc/yum.repos.d/elastic-beats.repo

[beats]

name=Elastic Beats Repository

baseurl=https://packages.elastic.co/beats/yum/el/$basearch

enabled=1

gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch

gpgcheck=1

### 安装filebeat

$ sudo yum -y install filebeat

或者

$ curl -L -O https://download.elastic.co/beats/filebeat/filebeat-1.2.2-x86\_64.rpm

$ sudo rpm -vi filebeat-1.2.2-x86\_64.rpm

注：rpm -qc filebeat查找filebeat核心配置文件为/etc/filebeat/filebeat.yml

### 配置Filebeat

Filebeat默认安装后其配置文件为/etc/filebeat/filebeat.yml。该配置文件遵从yaml语法格式。有较强的缩进等语法。可使用下列网站进行校验

<http://yaml-online-parser.appspot.com/><http://www.yamllint.com/>

#### [一个简单的配置](http://www.yamllint.com/)

##### [使用elasticsearch作为输出](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- "/var/log/\*.log"](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[elasticsearch:](http://www.yamllint.com/)

[hosts: ["192.168.0.228:9200"]](http://www.yamllint.com/)

[以上配置表示filebeat收集/var/log/目录下所有以.log结尾的日志文件，输出到elasticsearch](http://www.yamllint.com/)

##### [使用logstash作为输出](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- "/var/log/\*.log"](http://www.yamllint.com/)

[document\_type: syslog](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[以上配置表示filebeat收集/var/log/目录下所有以.log结尾的日志文件，输出到logstash。其中document\_type为之前在logstash中/etc/logstash/conf.d/10-syslog-filter.conf中定义的type类型。5044端口为之前在/etc/logstash/conf.d/02-beats-input.conf中为beats定义的port。certificate\_authorities同理，不再赘述。](http://www.yamllint.com/)

### [load filebeat template](http://www.yamllint.com/)

[$ curl -XPUT 'http://192.168.0.228:9200/\_template/filebeat' -d@/etc/filebeat/filebeat.template.json](http://www.yamllint.com/)

[返回{"acknowledged":true}则表示成功。](http://www.yamllint.com/)

[删除filebeat template](http://www.yamllint.com/)

[$ curl -XDELETE 'http://192.168.0.228:9200/filebeat-\*'](http://www.yamllint.com/)

[其中192.168.0.228:9200为elasticsearch服务。](http://www.yamllint.com/)

### [启动filebeat并添加为系统开机自启动服务](http://www.yamllint.com/)

[$ sudo systemctl start filebeat](http://www.yamllint.com/)

[$ sudo systemctl enable filebeat](http://www.yamllint.com/)

### [测试filebeat](http://www.yamllint.com/)

[$ curl -XGET 'http://192.168.0.228:9200/filebeat-\*/\_search?pretty'](http://www.yamllint.com/)

[{](http://www.yamllint.com/)

["took" : 2,](http://www.yamllint.com/)

["timed\_out" : false,](http://www.yamllint.com/)

["\_shards" : {](http://www.yamllint.com/)

["total" : 5,](http://www.yamllint.com/)

["successful" : 5,](http://www.yamllint.com/)

["failed" : 0](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["hits" : {](http://www.yamllint.com/)

["total" : 1159,](http://www.yamllint.com/)

["max\_score" : 1.0,](http://www.yamllint.com/)

["hits" : [ {](http://www.yamllint.com/)

["\_index" : "filebeat-2016.05.17",](http://www.yamllint.com/)

["\_type" : "syslog",](http://www.yamllint.com/)

["\_id" : "AVS8XSsvMXchSyg0mTVB",](http://www.yamllint.com/)

["\_score" : 1.0,](http://www.yamllint.com/)

["\_source" : {](http://www.yamllint.com/)

["message" : "May 16 21:35:11 c1 journal: Journal started",](http://www.yamllint.com/)

["@version" : "1",](http://www.yamllint.com/)

["@timestamp" : "2016-05-17T01:35:11.000Z",](http://www.yamllint.com/)

["source" : "/var/log/messages",](http://www.yamllint.com/)

["input\_type" : "log",](http://www.yamllint.com/)

["type" : "syslog",](http://www.yamllint.com/)

["count" : 1,](http://www.yamllint.com/)

["fields" : null,](http://www.yamllint.com/)

["beat" : {](http://www.yamllint.com/)

["hostname" : "c1",](http://www.yamllint.com/)

["name" : "c1"](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["offset" : 527932,](http://www.yamllint.com/)

["host" : "c1",](http://www.yamllint.com/)

["tags" : [ "beats\_input\_codec\_plain\_applied" ],](http://www.yamllint.com/)

["syslog\_timestamp" : "May 16 21:35:11",](http://www.yamllint.com/)

["syslog\_hostname" : "c1",](http://www.yamllint.com/)

["syslog\_program" : "journal",](http://www.yamllint.com/)

["syslog\_message" : "Journal started",](http://www.yamllint.com/)

["received\_at" : "2016-05-17T01:36:06.259Z",](http://www.yamllint.com/)

["received\_from" : "c1",](http://www.yamllint.com/)

["syslog\_severity\_code" : 5,](http://www.yamllint.com/)

["syslog\_facility\_code" : 1,](http://www.yamllint.com/)

["syslog\_facility" : "user-level",](http://www.yamllint.com/)

["syslog\_severity" : "notice"](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}]](http://www.yamllint.com/)

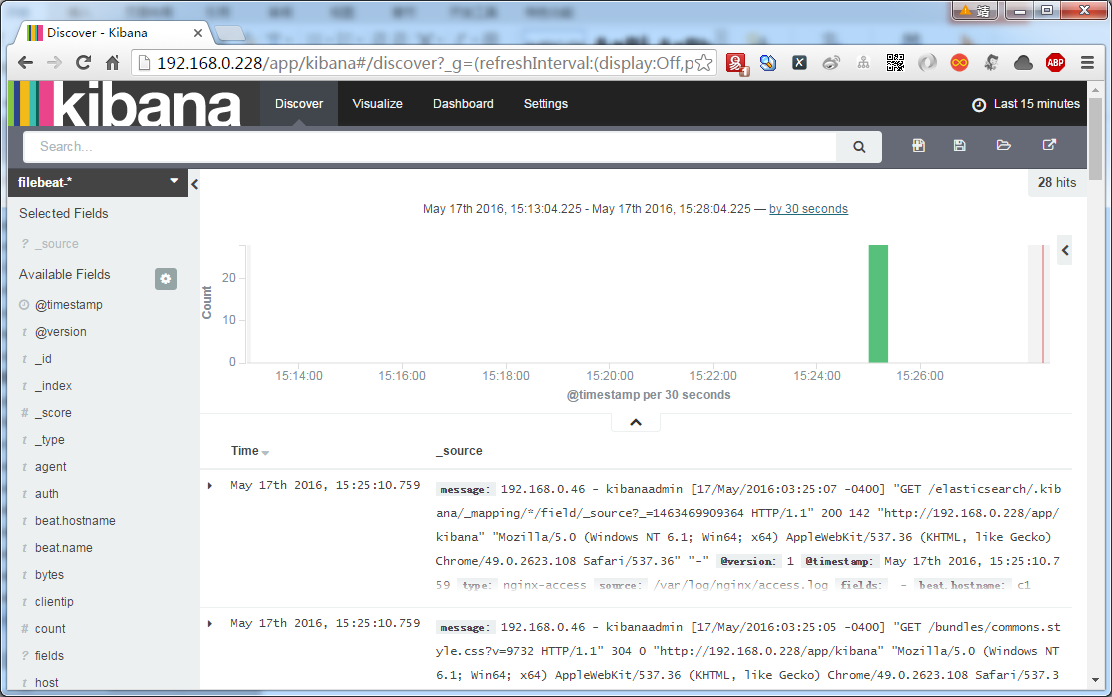
[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[观察控制台输出，若有结果输出则表示配置成功，否则仔细检查配置。](http://www.yamllint.com/)

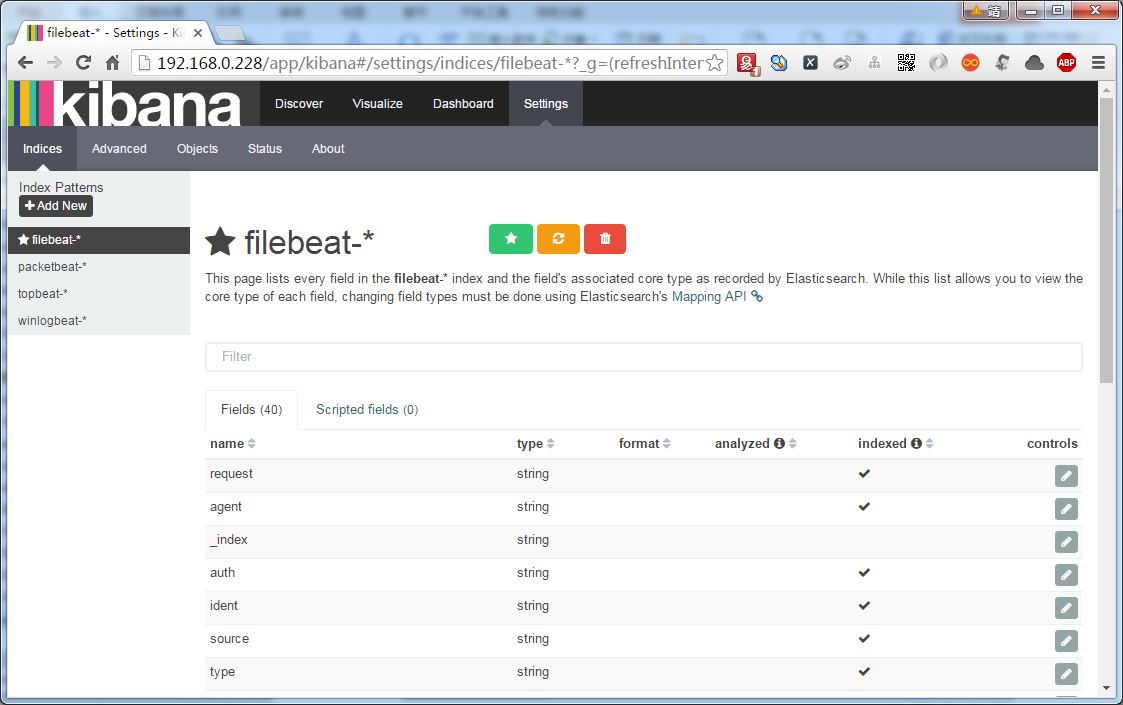
### [Connect to Kibana](http://www.yamllint.com/)

[http://192.168.0.228/会要求输入用户名密码，输入之前设置的kibanaadmin/kibanaadmin后，会反向代理到http://192.168.0.228/app/kibana](http://www.yamllint.com/)

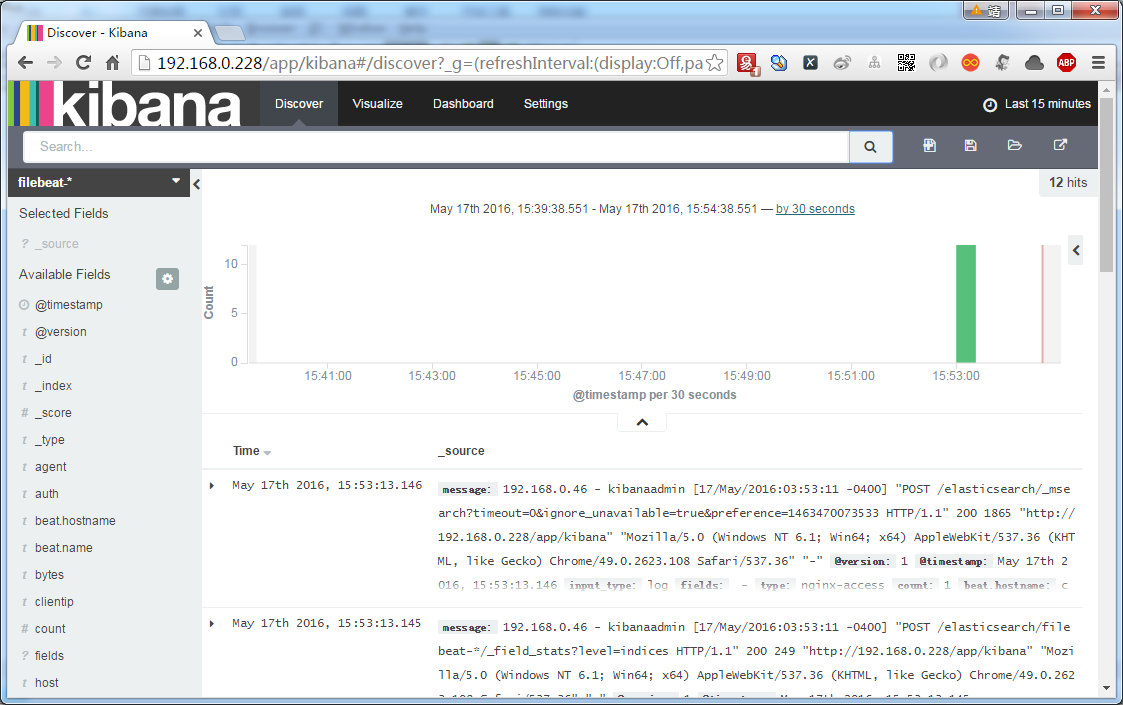
[[](http://www.yamllint.com/)](http://www.yamllint.com/)

[第一次请求系统要求设置一个默认的index pattern。这里默认设置filebeat-\*为默认。](http://www.yamllint.com/)

[依次点Settings->filebeat- ->★ 即可。](http://www.yamllint.com/)

[[](http://www.yamllint.com/)](http://www.yamllint.com/)

[Discover](http://www.yamllint.com/)

[[](http://www.yamllint.com/)](http://www.yamllint.com/)

## [安装topbeat](http://www.yamllint.com/)

[https://www.elastic.co/guide/en/beats/topbeat/current/index.html](http://www.yamllint.com/)

### [导入elasticsearch公钥](http://www.yamllint.com/)

[$ sudo rpm --import http://packages.elastic.co/GPG-KEY-elasticsearch](http://www.yamllint.com/)

### [创建elastic-beats.repo](http://www.yamllint.com/)

[$ sudo vim /etc/yum.repos.d/elastic-beats.repo](http://www.yamllint.com/)

[[beats]](http://www.yamllint.com/)

[name=Elastic Beats Repository](http://www.yamllint.com/)

[baseurl=https://packages.elastic.co/beats/yum/el/$basearch](http://www.yamllint.com/)

[enabled=1](http://www.yamllint.com/)

[gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch](http://www.yamllint.com/)

[gpgcheck=1](http://www.yamllint.com/)

### [安装topbeat](http://www.yamllint.com/)

[$ sudo yum -y install topbeat](http://www.yamllint.com/)

[或](http://www.yamllint.com/)

[$ curl -L -O https://download.elastic.co/beats/topbeat/topbeat-1.2.2-x86\_64.rpm](http://www.yamllint.com/)

[$ sudo rpm -vi topbeat-1.2.2-x86\_64.rpm](http://www.yamllint.com/)

[注：rpm -qc topbeat 查找topbeat核心配置文件为/etc/topbeat/topbeat.yml](http://www.yamllint.com/)

### [配置Topbeat](http://www.yamllint.com/)

[$ sudo vim /etc/topbeat/topbeat.yml](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[hosts: ["192.168.0.228:5044"]](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities: ["/etc/pki/tls/certs/logstash-forwarder.crt"]](http://www.yamllint.com/)

[这里配置同filebeat不再赘述。](http://www.yamllint.com/)

### [load topbeat template](http://www.yamllint.com/)

[$ curl -XPUT 'http://192.168.0.228:9200/\_template/topbeat' -d@/etc/topbeat/topbeat.template.json](http://www.yamllint.com/)

[返回{"acknowledged":true}则表示成功。](http://www.yamllint.com/)

[删除topbeat template](http://www.yamllint.com/)

[$ curl -XDELETE 'http://192.168.0.228:9200/topbeat-\*'](http://www.yamllint.com/)

[其中192.168.0.228:9200为elasticsearch服务。](http://www.yamllint.com/)

### [启动topbeat并添加为系统开机自启动服务](http://www.yamllint.com/)

[$ sudo systemctl restart topbeat](http://www.yamllint.com/)

[$ sudo systemctl enable topbeat](http://www.yamllint.com/)

### [测试topbeat](http://www.yamllint.com/)

[$ curl -XGET 'http://192.168.0.228:9200/topbeat-\*/\_search?pretty'](http://www.yamllint.com/)

[{](http://www.yamllint.com/)

["took" : 8,](http://www.yamllint.com/)

["timed\_out" : false,](http://www.yamllint.com/)

["\_shards" : {](http://www.yamllint.com/)

["total" : 5,](http://www.yamllint.com/)

["successful" : 5,](http://www.yamllint.com/)

["failed" : 0](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["hits" : {](http://www.yamllint.com/)

["total" : 277442,](http://www.yamllint.com/)

["max\_score" : 1.0,](http://www.yamllint.com/)

["hits" : [ {](http://www.yamllint.com/)

["\_index" : "topbeat-2016.05.17",](http://www.yamllint.com/)

["\_type" : "system",](http://www.yamllint.com/)

["\_id" : "AVS8XHQPMXchSyg0mTFD",](http://www.yamllint.com/)

["\_score" : 1.0,](http://www.yamllint.com/)

["\_source" : {](http://www.yamllint.com/)

["@timestamp" : "2016-05-17T01:37:26.228Z",](http://www.yamllint.com/)

["type" : "system",](http://www.yamllint.com/)

["load" : {](http://www.yamllint.com/)

["load1" : 4.07,](http://www.yamllint.com/)

["load5" : 1.8,](http://www.yamllint.com/)

["load15" : 0.68](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["cpu" : {](http://www.yamllint.com/)

["user" : 3126,](http://www.yamllint.com/)

["user\_p" : 0.0293,](http://www.yamllint.com/)

["nice" : 3190,](http://www.yamllint.com/)

["system" : 2627,](http://www.yamllint.com/)

["system\_p" : 0.0984,](http://www.yamllint.com/)

["idle" : 156,](http://www.yamllint.com/)

["iowait" : 2322,](http://www.yamllint.com/)

["irq" : 0,](http://www.yamllint.com/)

["softirq" : 485,](http://www.yamllint.com/)

["steal" : 0](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["mem" : {](http://www.yamllint.com/)

["total" : 3009445888,](http://www.yamllint.com/)

["used" : 948916224,](http://www.yamllint.com/)

["free" : 2060529664,](http://www.yamllint.com/)

["used\_p" : 0.32,](http://www.yamllint.com/)

["actual\_used" : 664776704,](http://www.yamllint.com/)

["actual\_free" : 2344669184,](http://www.yamllint.com/)

["actual\_used\_p" : 0.22](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["swap" : {](http://www.yamllint.com/)

["total" : 1610608640,](http://www.yamllint.com/)

["used" : 0,](http://www.yamllint.com/)

["free" : 1610608640,](http://www.yamllint.com/)

["used\_p" : 0](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["count" : 1,](http://www.yamllint.com/)

["beat" : {](http://www.yamllint.com/)

["hostname" : "c1",](http://www.yamllint.com/)

["name" : "c1"](http://www.yamllint.com/)

[},](http://www.yamllint.com/)

["@version" : "1",](http://www.yamllint.com/)

["host" : "c1",](http://www.yamllint.com/)

["tags" : [ "beats\_input\_raw\_event" ]](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}]](http://www.yamllint.com/)

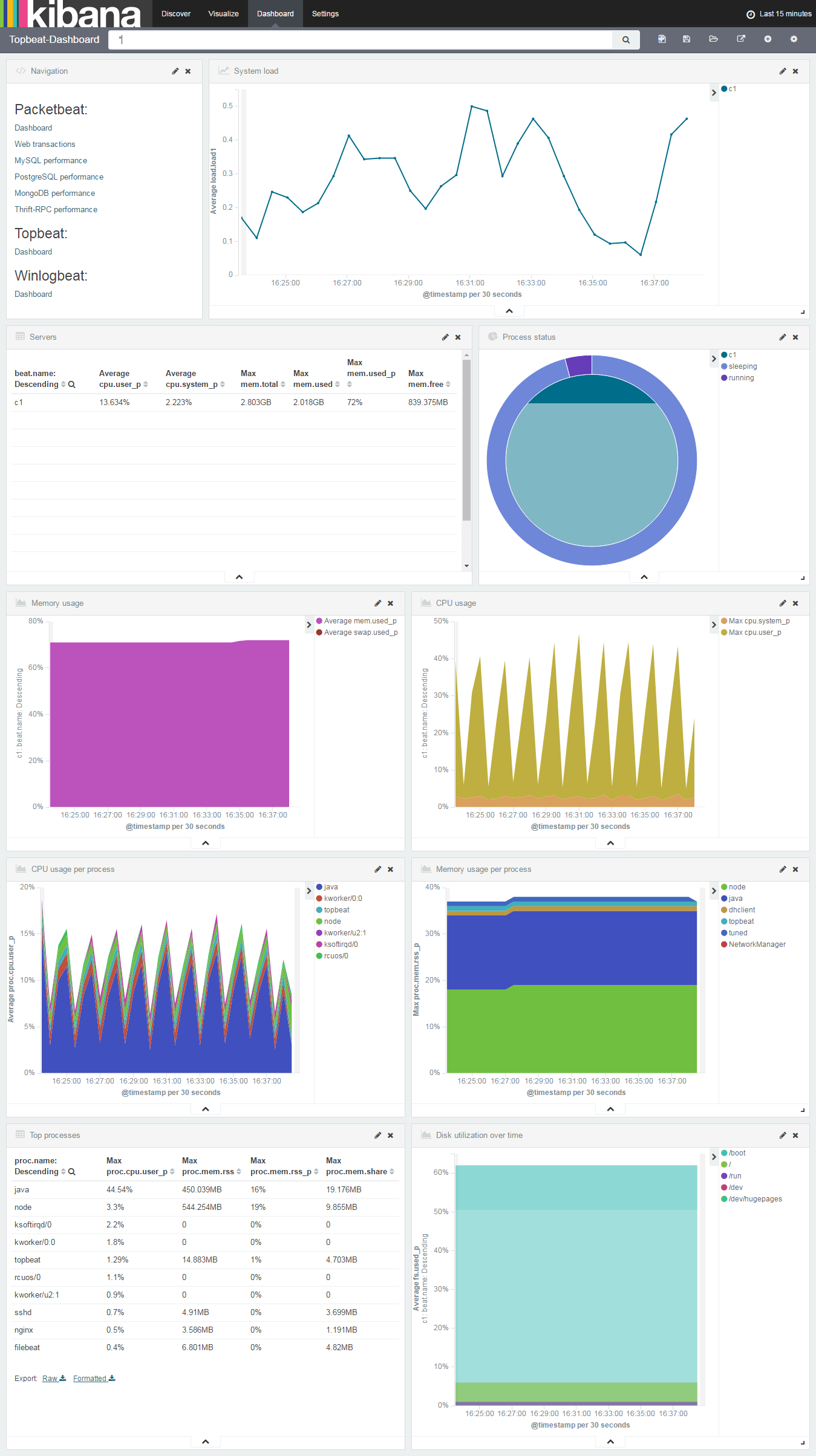
[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[返回类似如上信息则表示配置成功。](http://www.yamllint.com/)

### [Connect to Kibana](http://www.yamllint.com/)

[使用Topbeat Dashboard](http://www.yamllint.com/)

[](http://www.yamllint.com/)

## [logstash扩展配置](http://www.yamllint.com/)

[首先得明确以下几点](http://www.yamllint.com/)

1. [logstash安装在/opt/logstash](http://www.yamllint.com/)
2. [logstash配置目录为/etc/logstash/conf.d](http://www.yamllint.com/)
3. [确定存在名为02-beats-input.conf配置文件，该文件在上文之前创建配置过](http://www.yamllint.com/)
4. [确定存在名为30-elasticsearch-output.conf配置文件，该文件在上文之前创建配置过](http://www.yamllint.com/)

[创建patterns](http://www.yamllint.com/)

[$ sudo mkdir -p /opt/logstash/patterns](http://www.yamllint.com/)

[$ sudo chown logstash: /opt/logstash/patterns](http://www.yamllint.com/)

[修改/etc/filebeat/filebeat.yml文件](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: syslog](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/secure](http://www.yamllint.com/)

[- /var/log/messages](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: sys-log](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/\*.log](http://www.yamllint.com/)

[registry\_file: /var/lib/filebeat/registry](http://www.yamllint.com/)

[logging:](http://www.yamllint.com/)

[files:](http://www.yamllint.com/)

[rotateeverybytes: 10485760](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[shipper: ~](http://www.yamllint.com/)

### [Nginx日志配置](http://www.yamllint.com/)

#### [Logstash Patterns: Nginx](http://www.yamllint.com/)

[$ sudo mkdir -p /opt/logstash/patterns](http://www.yamllint.com/)

[sudo vim /opt/logstash/patterns/nginx](http://www.yamllint.com/)

[NGUSERNAME [a-zA-Z\.\@\-\+\_%]+](http://www.yamllint.com/)

[NGUSER %{NGUSERNAME}](http://www.yamllint.com/)

[NGINXACCESS %{IPORHOST:clientip} %{NGUSER:ident} %{NGUSER:auth} \[%{HTTPDATE:timestamp}\] "%{WORD:verb} %{URIPATHPARAM:request} HTTP/%{NUMBER:httpversion}" %{NUMBER:response} (?:%{NUMBER:bytes}|-) (?:"(?:%{URI:referrer}|-)"|%{QS:referrer}) %{QS:agent}](http://www.yamllint.com/)

[$ sudo chown logstash: /opt/logstash/patterns/nginx](http://www.yamllint.com/)

#### [Logstash Filter: Nginx](http://www.yamllint.com/)

[$ sudo vim /etc/logstash/conf.d/11-nginx-filter.conf](http://www.yamllint.com/)

[filter {](http://www.yamllint.com/)

[if [type] == "nginx-access" {](http://www.yamllint.com/)

[grok {](http://www.yamllint.com/)

[match => { "message" => "%{NGINXACCESS}" }](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

#### [重启logstash](http://www.yamllint.com/)

[$ sudo service logstash restart](http://www.yamllint.com/)

#### [Filebeat Prospector: Nginx](http://www.yamllint.com/)

[修改/etc/filebeat/filebeat.yml配置](http://www.yamllint.com/)

[$ sudo vim /etc/filebeat/filebeat.yml](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: nginx-access](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/nginx/access.log](http://www.yamllint.com/)

[registry\_file: /var/lib/filebeat/registry](http://www.yamllint.com/)

[logging:](http://www.yamllint.com/)

[files:](http://www.yamllint.com/)

[rotateeverybytes: 10485760](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

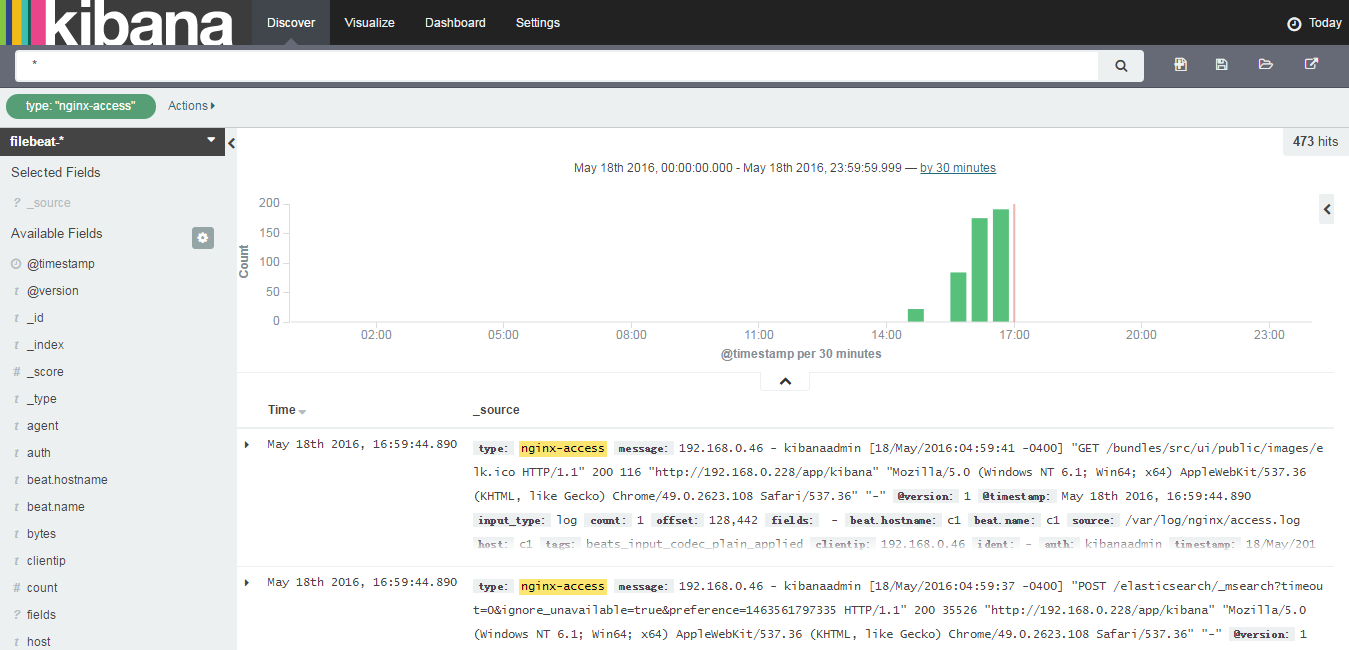
[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[shipper: ~](http://www.yamllint.com/)

#### [重启filebeat](http://www.yamllint.com/)

[$ sudo service filebeat restart](http://www.yamllint.com/)

#### [kibana搜索效果图](http://www.yamllint.com/)

[](http://www.yamllint.com/)

### [Apache HTTP Web Server日志配置](http://www.yamllint.com/)

#### [Logstash Filter: Apache](http://www.yamllint.com/)

[$ sudo vi /etc/logstash/conf.d/12-apache.conf](http://www.yamllint.com/)

[filter {](http://www.yamllint.com/)

[if [type] == "apache-access" {](http://www.yamllint.com/)

[grok {](http://www.yamllint.com/)

[match => { "message" => "%{COMBINEDAPACHELOG}" }](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

#### [重启logstash](http://www.yamllint.com/)

[$ sudo service logstash restart](http://www.yamllint.com/)

#### [Filebeat Prospector: Apache](http://www.yamllint.com/)

[$ sudo vim /etc/filebeat/filebeat.yml](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: apache-access](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/apache2/access.log](http://www.yamllint.com/)

[registry\_file: /var/lib/filebeat/registry](http://www.yamllint.com/)

[logging:](http://www.yamllint.com/)

[files:](http://www.yamllint.com/)

[rotateeverybytes: 10485760](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[shipper: ~](http://www.yamllint.com/)

#### [重启filebeat](http://www.yamllint.com/)

[sudo service filebeat restart](http://www.yamllint.com/)

### [Tomcat日志配置](http://www.yamllint.com/)

[参考链接](http://www.yamllint.com/)

[http://blog.kazaff.me/2015/06/05/%E6%97%A5%E5%BF%97%E6%94%B6%E9%9B%86%E6%9E%B6%E6%9E%84--ELK/](http://www.yamllint.com/)

[https://aggarwalarpit.wordpress.com/2015/12/03/configuring-elk-stack-to-analyse-apache-tomcat-logs/](http://www.yamllint.com/)

[https://www.systemcodegeeks.com/web-servers/apache/configuring-elk-stack-analyse-apache-tomcat-logs/](http://www.yamllint.com/)

[http://stackoverflow.com/questions/25429377/how-can-i-integrate-tomcat6s-catalina-out-file-with-logstash-elasticsearch](http://www.yamllint.com/)

[https://blog.codecentric.de/en/2014/10/log-management-spring-boot-applications-logstash-elastichsearch-kibana/](http://www.yamllint.com/)

[https://github.com/sdd330/tomcat-elk](http://www.yamllint.com/)

[https://blog.lanyonm.org/articles/2014/01/12/logstash-multiline-tomcat-log-parsing.html](http://www.yamllint.com/)

[https://spredzy.wordpress.com/2013/03/02/monitor-your-cluster-of-tomcat-applications-with-logstash-and-kibana/](http://www.yamllint.com/)

#### [定义Logstash Patterns: Tomcat](http://www.yamllint.com/)

[$ vim /opt/logstash/patterns/tomcat](http://www.yamllint.com/)

[JAVACLASS (?:[a-zA-Z0-9-]+\.)+[A-Za-z0-9$]+](http://www.yamllint.com/)

[JAVALOGMESSAGE (.\*)](http://www.yamllint.com/)

[# MMM dd, yyyy HH:mm:ss eg: Jan 9, 2014 7:13:13 AM](http://www.yamllint.com/)

[CATALINA\_DATESTAMP %{MONTH} %{MONTHDAY}, 20%{YEAR} %{HOUR}:?%{MINUTE}(?::?%{SECOND}) (?:AM|PM)](http://www.yamllint.com/)

[# yyyy-MM-dd HH:mm:ss,SSS ZZZ eg: 2014-01-09 17:32:25,527 -0800](http://www.yamllint.com/)

[TOMCAT\_DATESTAMP 20%{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{HOUR}:?%{MINUTE}(?::?%{SECOND}) %{ISO8601\_TIMEZONE}](http://www.yamllint.com/)

[CATALINALOG %{CATALINA\_DATESTAMP:timestamp} %{JAVACLASS:class} %{JAVALOGMESSAGE:logmessage}](http://www.yamllint.com/)

[# 2014-01-09 20:03:28,269 -0800 | ERROR | com.example.service.ExampleService - something compeletely unexpected happened...](http://www.yamllint.com/)

[TOMCATLOG %{TOMCAT\_DATESTAMP:timestamp} \| %{LOGLEVEL:level} \| %{JAVACLASS:class} - %{JAVALOGMESSAGE:logmessage}](http://www.yamllint.com/)

#### [定义Logstash Filter: Tomcat](http://www.yamllint.com/)

[$ vim /etc/logstash/conf.d/13-tomcat.conf](http://www.yamllint.com/)

[filter {](http://www.yamllint.com/)

[if [type] == "tomcat\_access" {](http://www.yamllint.com/)

[grok {](http://www.yamllint.com/)

[match => [ "message", "%{TOMCATLOG}", "message", "%{CATALINALOG}" ]](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[date {](http://www.yamllint.com/)

[match => [ "timestamp", "yyyy-MM-dd HH:mm:ss,SSS Z", "MMM dd, yyyy HH:mm:ss a" ]](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

[}](http://www.yamllint.com/)

#### [重启logstash](http://www.yamllint.com/)

[$ sudo service logstash restart](http://www.yamllint.com/)

#### [Filebeat Prospector: Tomcat](http://www.yamllint.com/)

[修改/etc/filebeat/filebeat.yml配置](http://www.yamllint.com/)

[$ sudo vim /etc/filebeat/filebeat.yml](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: tomcat-access](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /home/vagrant/tomcat-7.0.69/logs/\*.log](http://www.yamllint.com/)

[registry\_file: /var/lib/filebeat/registry](http://www.yamllint.com/)

[logging:](http://www.yamllint.com/)

[files:](http://www.yamllint.com/)

[rotateeverybytes: 10485760](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

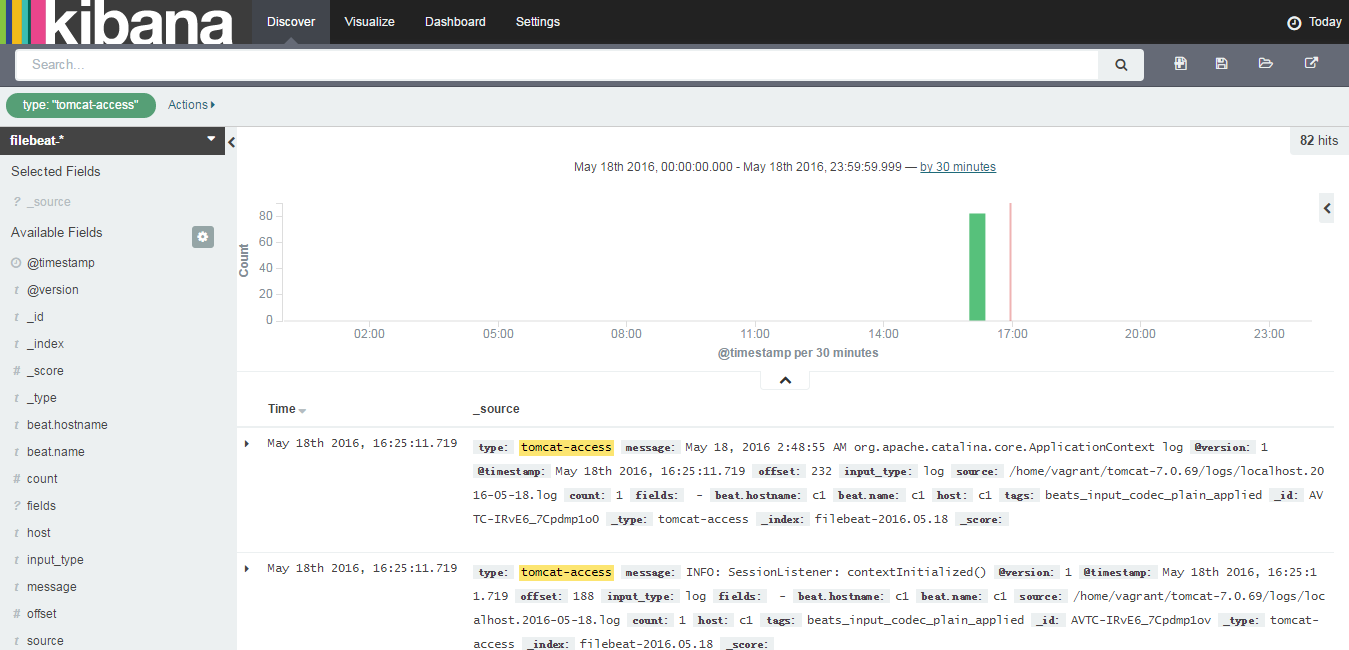
[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[shipper: ~](http://www.yamllint.com/)

#### [重启filebeat](http://www.yamllint.com/)

[$ sudo service filebeat restart](http://www.yamllint.com/)

#### [kibana搜索效果图](http://www.yamllint.com/)

[](http://www.yamllint.com/)

### [最终配置](http://www.yamllint.com/)

[/etc/filebeat/filebeat.yml集各配置于一体的一个最终配置如下：](http://www.yamllint.com/)

[---](http://www.yamllint.com/)

[filebeat:](http://www.yamllint.com/)

[prospectors:](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: syslog](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/secure](http://www.yamllint.com/)

[- /var/log/messages](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: sys-log](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/\*.log](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: nginx-access](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/nginx/access.log](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: apache-access](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /var/log/apache2/access.log](http://www.yamllint.com/)

[-](http://www.yamllint.com/)

[document\_type: tomcat-access](http://www.yamllint.com/)

[input\_type: log](http://www.yamllint.com/)

[paths:](http://www.yamllint.com/)

[- /home/vagrant/tomcat-7.0.69/logs/\*.log](http://www.yamllint.com/)

[registry\_file: /var/lib/filebeat/registry](http://www.yamllint.com/)

[logging:](http://www.yamllint.com/)

[files:](http://www.yamllint.com/)

[rotateeverybytes: 10485760](http://www.yamllint.com/)

[output:](http://www.yamllint.com/)

[logstash:](http://www.yamllint.com/)

[bulk\_max\_size: 1024](http://www.yamllint.com/)

[hosts:](http://www.yamllint.com/)

[- "192.168.0.228:5044"](http://www.yamllint.com/)

[tls:](http://www.yamllint.com/)

[certificate\_authorities:](http://www.yamllint.com/)

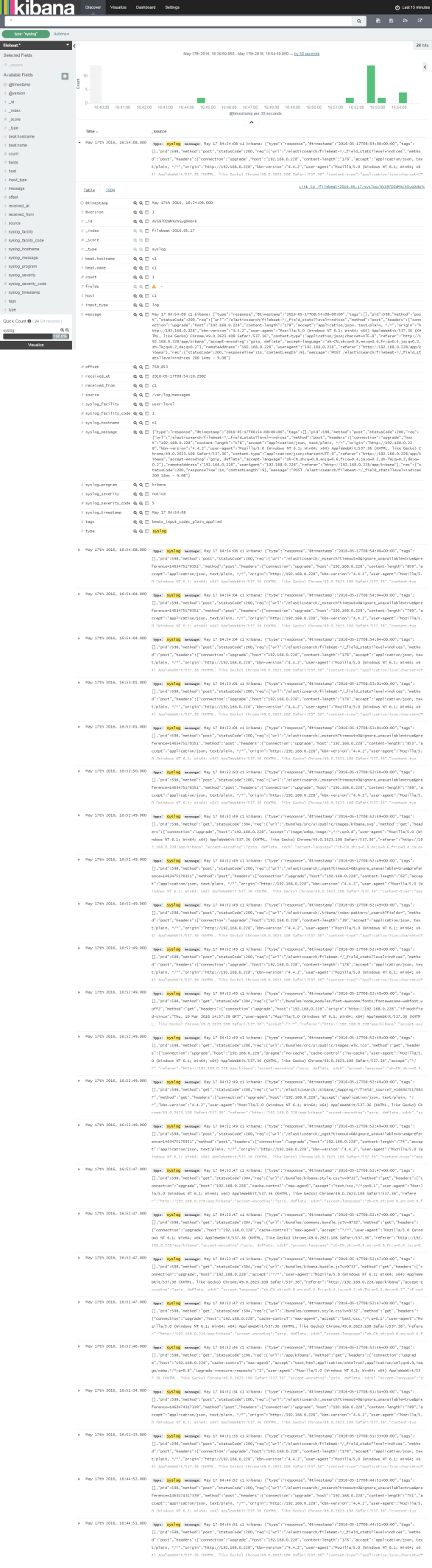
[- /etc/pki/tls/certs/logstash-forwarder.crt](http://www.yamllint.com/)

[shipper: ~](http://www.yamllint.com/)

## 使用Kibana查询分析日志

这里注意涉及Discover、Visualize、Dashboard、Settings面板的使用。具体用法请结合官方文档。这里不再赘述。

系统日志



Nginx日志



## Elasticsearch插件安装

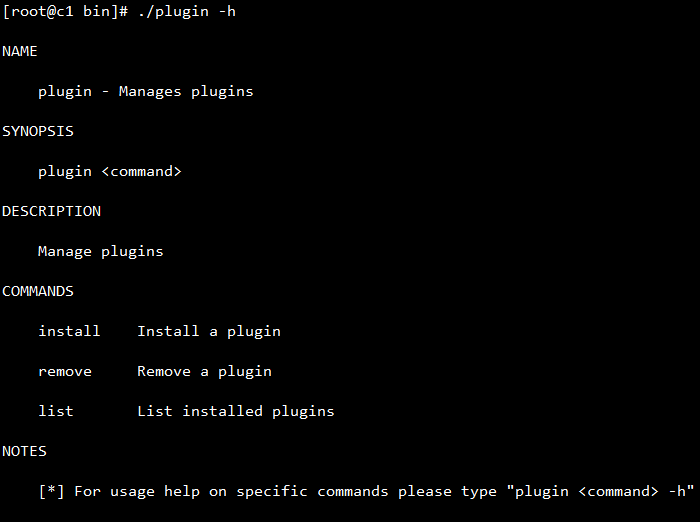
<https://www.elastic.co/guide/en/elasticsearch/plugins/current/installation.html>

### plugin命令介绍

Elasticsearch默认安装在/usr/share/elasticsearch路径下

进入到/usr/share/elasticsearch/bin目录。使用该目录下的plugin命令管理插件

使用./plugin -h命令会列出plugin命令选项的提示信息

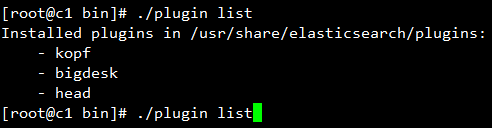


./plugin install #安装插件

./plugin remove #移除插件

./plugin list #列出已安装插件列表

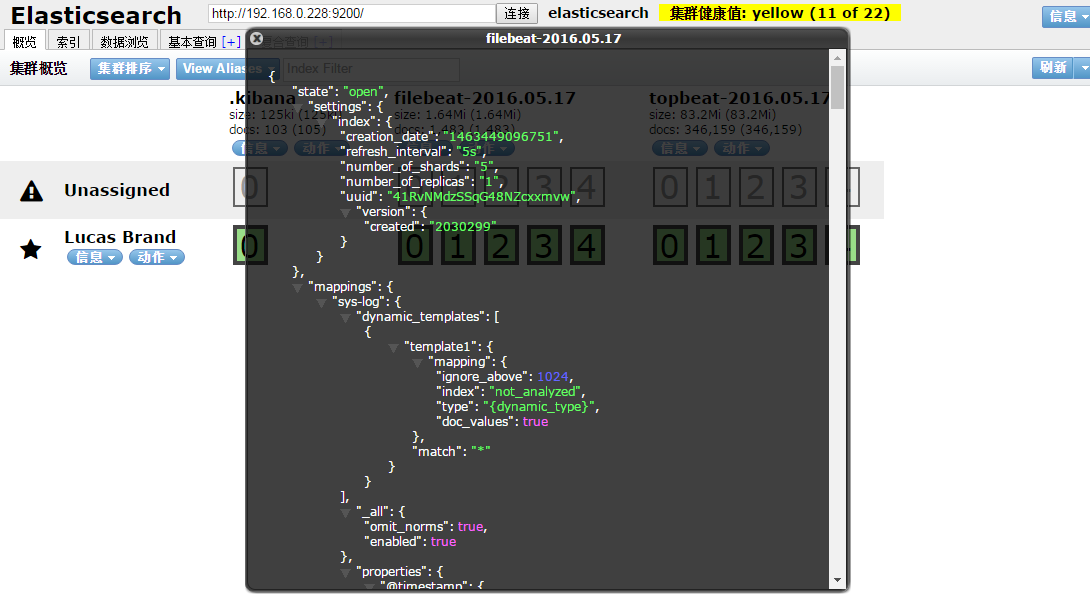
这里列出我常用的也是功能最为强大的三款插件

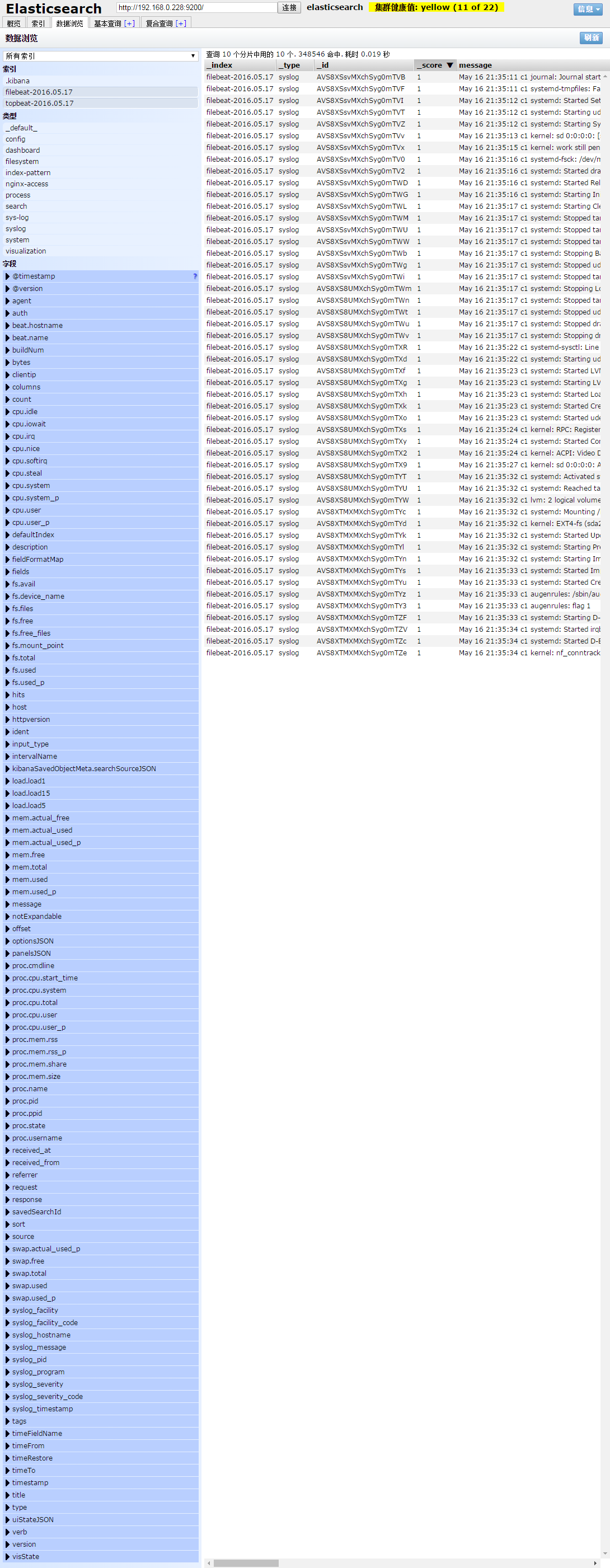


### 安装head插件

$ sudo /usr/share/elasticsearch/bin/plugin install mobz/elasticsearch-head

访问http://192.168.0.228:9200/\_plugin/head/

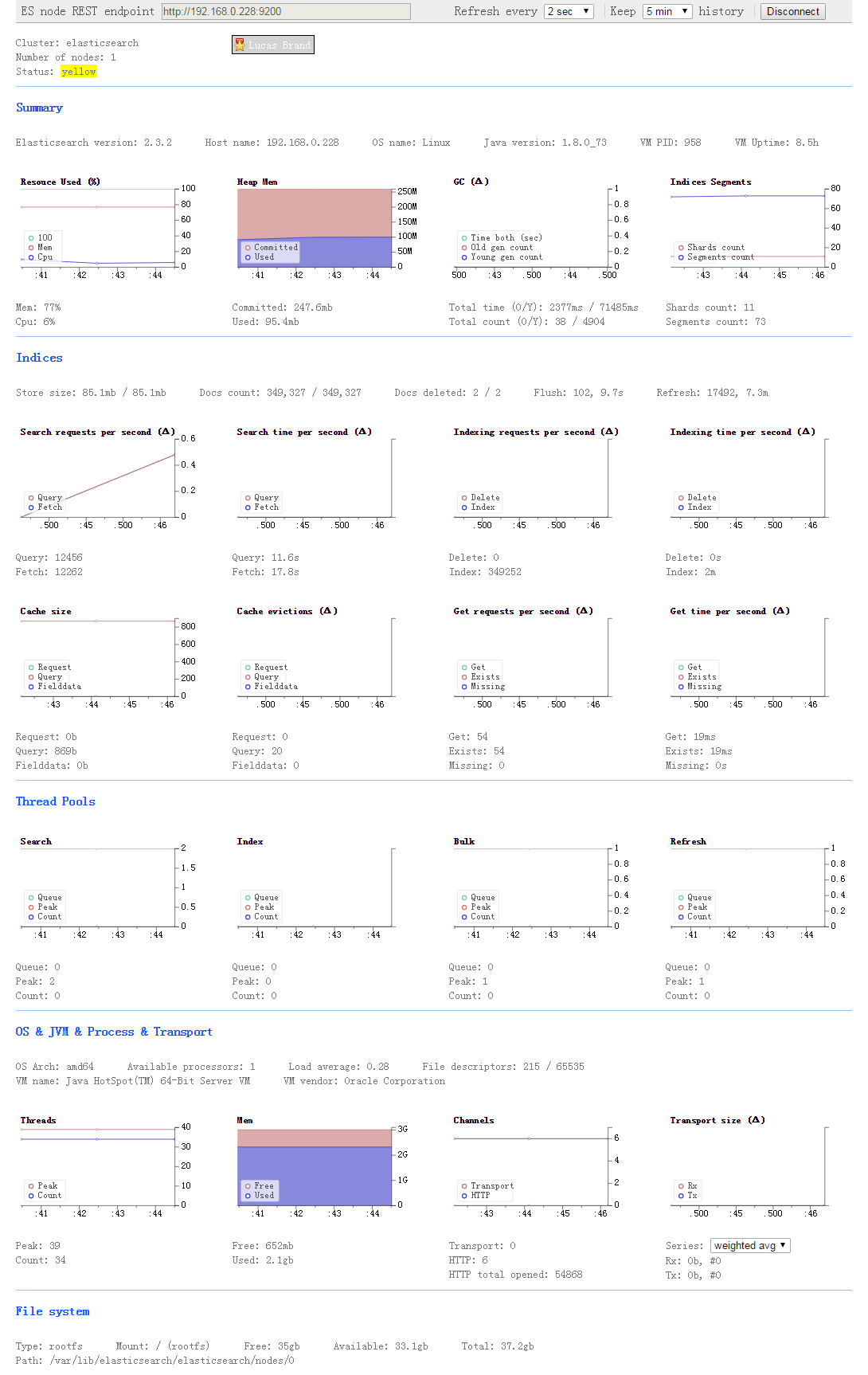




### 安装bigdesk插件

$ sudo /usr/share/elasticsearch/bin/plugin install lukas-vlcek/bigdesk/2.5.0

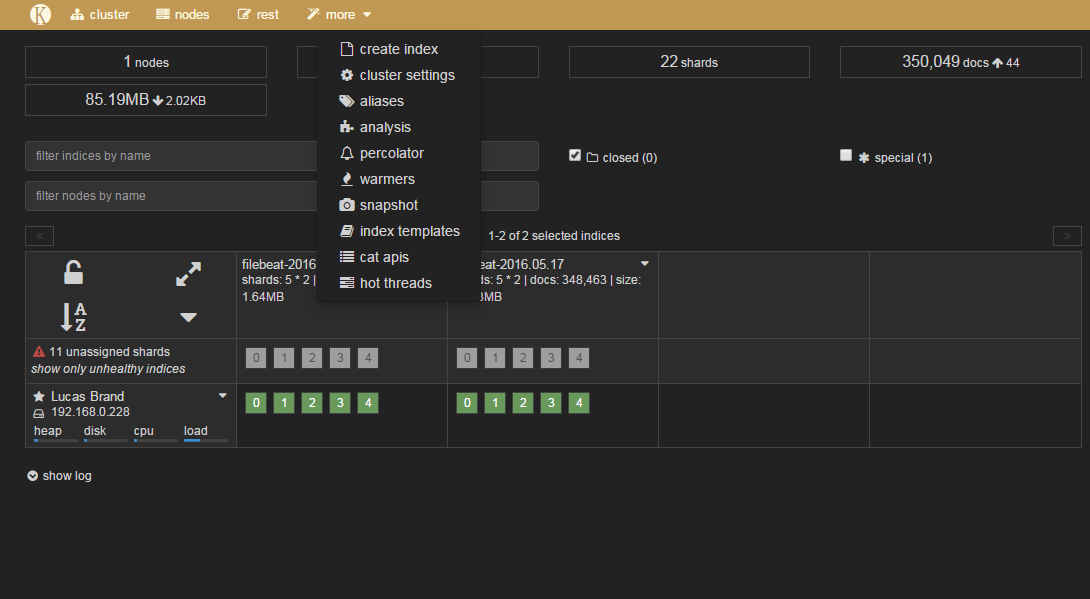
访问http://192.168.0.228:9200/\_plugin/bigdesk/



### 安装kopf插件

$ sudo /usr/share/elasticsearch/bin/plugin install lmenezes/elasticsearch-kopf/2.1.2

访问http://192.168.0.228:9200/\_plugin/kopf/



### 插件列表

https://www.elastic.co/guide/en/elasticsearch/plugins/current/management.html

https://www.elastic.co/guide/en/elasticsearch/plugins/current/integrations.html

# 参考资料

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-7>

<https://www.digitalocean.com/community/tutorials/how-to-gather-infrastructure-metrics-with-topbeat-and-elk-on-centos-7>

<https://www.digitalocean.com/community/tutorials/adding-logstash-filters-to-improve-centralized-logging>

<https://www.digitalocean.com/community/tutorials/how-to-use-kibana-dashboards-and-visualizations>

<https://www.digitalocean.com/community/tutorials/how-to-map-user-location-with-geoip-and-elk-elasticsearch-logstash-and-kibana>

# 使用Elasticsearch做全文检索

当使用elasticsearch搜索中文时就需要安装中文分词器。

关于elasticsearch更多内容可参阅

<https://github.com/sxyx2008/elasticsearch> elasticsearch中文版，基于elasticsearch-1.7.1。集成常用的各种插件

<https://github.com/sxyx2008/elasticsearch-jest-example> ElasticSearch Java API编程接口

<https://github.com/sxyx2008/elasticsearch/issues/2> elasticsearch analysis ansj分词器的安装及使用

<https://github.com/sxyx2008/elasticsearch/issues/3> elasticsearch-jdbc插件的使用

<https://github.com/sxyx2008/elasticsearch/issues/5> elasticsearch rest api快速上手