QQ截图20151201103408.png

**ELK日志服务器搭建手册**

信息技术中心

2016年11月13日

**文档修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 日 期 | 版本 | 描述信息 | 作者 |
| 2016-11-13 | 1.0 | 新建 | 陈俊彦 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 前言

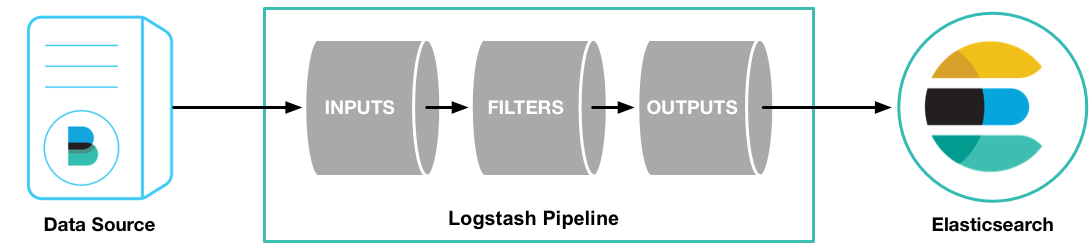
ELK 由 ElasticSearch 、 Logstash 和 Kiabana 三个开源工具组成。官方网站：https://www.elastic.co

其中的3个软件是：

Elasticsearch 是个开源分布式搜索引擎，它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制， restful 风格接口，多数据源，自动搜索负载等。

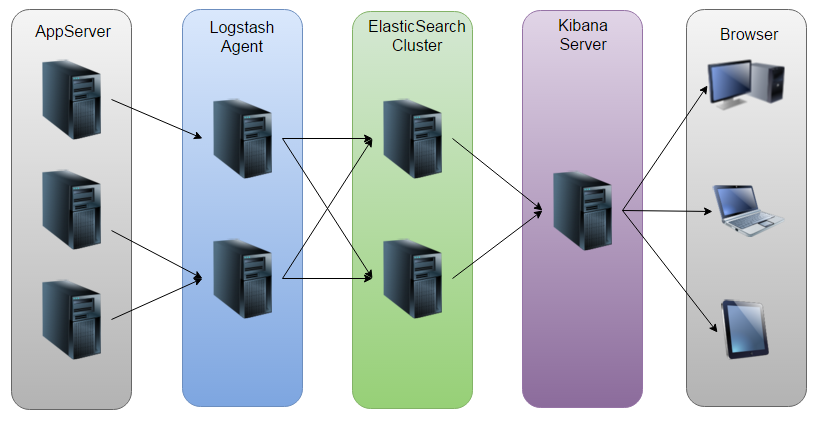
Logstash 是一个完全开源的工具，他可以对你的日志进行收集、分析，并将其存储供以后使用（如，搜索）。

A Logstash pipeline has two required elements, input and output, and one optional element,filter. The input plugins consume data from a source, the filter plugins modify the data as you specify, and the output plugins write the data to a destination.



kibana 也是一个开源和免费的工具，他 Kibana 可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助您汇总、分析和搜索重要数据日志

ELK工作的原理图：



如图：Logstash收集AppServer产生的Log，并存放到ElasticSearch集群中，而Kibana则从ES集群中查询数据生成图表，再返回给Browser。

# 环境准备

2.1 主机信息

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 操作系统 | 主机名 | 硬件配置 | 应用软件信息 | IP | 用途 |
| 1 | CenOS 7.2 | D2-ELK21 | 4 Vcpu  16G Memory | elasticsearch-5.0  JDK 1.8.0\_112 | 10.163.36.21 | 后端日志数据存储 |
| 2 | CenOS 7.2 | D2-ELK22 | 8 Vcpu  32G Memory | JDK 1.8.0\_112 | 10.163.36.22 | 前端数据收集和显示 |
| 3 | CenOS 7.2 |  | 4 Vcpu  8G Memory | JDK 1.8.0\_112 |  | 客户端 |

2.2 关闭服务器端防火墙和SELinux

$ /etc/init.d/iptables stop

$ setenforce 0

这里我们为了不影响模块之间的相互通信，暂时先把几台设备的iptables都关闭了。

# 部署和配置JDK

在ELK环境（D2-ELK21和D2-ELK22）安装配置JDK环境

### 3.1安装JDK

下载jdk包： jdk-8u112-linux-x64.tar.gz保存至/app/java目录

执行$ tar zxvf jdk-8u112-linux-x64.tar.gz将其进行解压

### 3.2 配置环境变量

$ vi /etc/profile

export JAVA\_HOME=/app/java/jdk1.8.0\_112

export JRE\_HOME=$JAVA\_HOME/jre

export CLASSPATH=.:$JAVA\_HOME/lib:$JRE\_HOME/lib:$CLASSPATH

export PATH=$PATH:$JAVA\_HOME/bin:$JRE\_HOME/bin

### 3.3 环境变量生效

运行$ source /etc/profile

运行$ java -version

# java -version

java version "1.8.0\_112"

Java(TM) SE Runtime Environment (build 1.8.0\_112-b15)

Java HotSpot(TM) 64-Bit Server VM (build 25.112-b15, mixed mode)

# 4 安装配置elasticsearch

在D2-ELK22安装elasticsearch

Elastisearch v5.0.0 下载地址

<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.0.1.tar.gz>

## 4.1 安装tar.gz包

mv elasticsearch-5.0.0.tar.gz /app/

tar zxvf elasticsearch-5.0.0.tar.gz

mv /app/elasticsearch-5.0.0 /app/elasticsearch

tar.gz安装的文件目录如下

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Description | Default Location | Setting |
| home | Elasticsearch home directory or $ES\_HOME | /app/elasticsearch |  |
| bin | Binary scripts including elasticsearch to start a node and elasticsearch-plugin to install plugins | $ES\_HOME/bin |  |
| conf | Configuration files including elasticsearch.yml | $ES\_HOME/config | path.conf |
| data | The location of the data files of each index / shard allocated on the node. Can hold multiple locations. | $ES\_HOME/data | path.data |
| logs | Log files location. | $ES\_HOME/logs | path.logs |
| plugins | Plugin files location. Each plugin will be contained in a subdirectory. | $ES\_HOME/plugins |  |
| repo | Shared file system repository locations. Can hold multiple locations. A file system repository can be placed in to any subdirectory of any directory specified here. | Not configured | path.repo |
| script | Location of script files. | $ES\_HOME/scripts | path.scripts |

## 4.2 安装配置X-Pack

### 4.2.1为elasticsearch手动下载X-Pack

<https://artifacts.elastic.co/downloads/packs/x-pack/x-pack-5.0.1.zip>

### 4.2.2手动安装X-Pack

关闭elasticsearch服务后，在每一个节点的Elasticsearch的安装目录下运行 bin/elasticsearch-plugin 安装X-Pack

# /app/elasticsearch/bin/elasticsearch-plugin install file:///home/gelcmw/x-pack-5.0.1.zip

-> Downloading file:///home/gelcmw/x-pack-5.0.1.zip

[=================================================] 100%

@ WARNING: plugin requires additional permissions @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

\* java.lang.RuntimePermission accessClassInPackage.com.sun.activation.registries

\* java.lang.RuntimePermission getClassLoader

\* java.lang.RuntimePermission setContextClassLoader

\* java.lang.RuntimePermission setFactory

\* java.security.SecurityPermission createPolicy.JavaPolicy

\* java.security.SecurityPermission getPolicy

\* java.security.SecurityPermission putProviderProperty.BC

\* java.security.SecurityPermission setPolicy

\* java.util.PropertyPermission \* read,write

\* java.util.PropertyPermission sun.nio.ch.bugLevel write

\* javax.net.ssl.SSLPermission setHostnameVerifier

See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html

for descriptions of what these permissions allow and the associated risks.

Continue with installation? [y/N]**y**

-> Installed x-pack

### 4.2.3启动X-Pack相关features

X-Pack相关features默认是启动的。

Elasticsearch通过elasticsearch.yml, kibana通过 kibana.yml启动、关闭X-Pack相关features

|  |  |
| --- | --- |
| Setting | Description |
| xpack.security.enabled | Set to false to disable X-Pack security. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.monitoring.enabled | Set to false to disable X-Pack monitoring. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.graph.enabled | Set to false to disable X-Pack graph. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.watcher.enabled | Set to false to disable Watcher. Configure in elasticsearch.yml only. |
| xpack.reporting.enabled | Set to false to disable X-Pack reporting. Configure in kibana.yml only. |

### 4.2.4 X-Pack提供以下几个级别保护elastic集群

用户验证授权和基于角色的访问控制节点/客户端认证和信道加密审计

#### 4.2.4.1启动消息身份验证，验证消息在传输的过程中未被篡改或者修改

# /app/elasticsearch/bin/x-pack/syskeygen

Storing generated key in [/app/elasticsearch/config/x-pack/system\_key]...

Ensure the generated key can be read by the user that Elasticsearch runs as, permissions are set to owner read/write only

如果es是一个集群，请将生成的密钥复制到集群的其他节点同一目录下

/app/elasticsearch/config/x-pack/system\_key

#### 4.2.4.2启动审核以跟踪与您的elasticsearch集群的尝试与成功的交互

配置/app/elasticsearch/config/elasticsearch.yml，添加xpack.security.audit.enabled启用审核

# vi /app/elasticsearch/config/elasticsearch.yml

xpack.security.audit.enabled: true

## 4.3 设置elasticsearch配置文件

### 4.3.1 配置/app/elasticsearch/config/elasticsearch.yml

Elasticsearch的默认配置文件在 /app/elasticsearch/config/elasticsearch.yml

The format of this config file is explained in

https://www.elastic.co/guide/en/elasticsearch/reference/5.0/important-settings.html

# cat /app/elasticsearch/config/elasticsearch.yml

# ======================== Elasticsearch Configuration =========================

# NOTE: Elasticsearch comes with reasonable defaults for most settings.

# Before you set out to tweak and tune the configuration, make sure you

# understand what are you trying to accomplish and the consequences.

# The primary way of configuring a node is via this file. This template lists

# the most important settings you may want to configure for a production cluster.

# Please see the documentation for further information on configuration options:

#<http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration.html>

# ---------------------------------- Cluster -----------------------------------

# Use a descriptive name for your cluster:

cluster.name: elk\_cluster

# ------------------------------------ Node ------------------------------------

# Use a descriptive name for the node:

node.name: D2-ELK22

# Add custom attributes to the node:

#node.attr.rack: r1

# ----------------------------------- Paths ------------------------------------

# Path to directory where to store the data (separate multiple locations by comma):

path.data: /app/elasticsearch/data

#

# Path to log files:

path.logs: /app/elasticsearch/logs

# ----------------------------------- Memory -----------------------------------

# Lock the memory on startup:

bootstrap.memory\_lock: true

# Make sure that the heap size is set to about half the memory available

# on the system and that the owner of the process is allowed to use this

# limit.

# Elasticsearch performs poorly when the system is swapping the memory.

# ---------------------------------- Network -----------------------------------

# Set the bind address to a specific IP (IPv4 or IPv6):

network.host: 10.163.36.22

# Set a custom port for HTTP:

http.port: 9200

# For more information, see the documentation at:

#http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-network.html>

# --------------------------------- Discovery ----------------------------------

# Pass an initial list of hosts to perform discovery when new node is started:

# The default list of hosts is ["127.0.0.1", "[::1]"]

#discovery.zen.ping.unicast.hosts: ["10.163.36.22:9300"]

#If only one node in the cluster, disable above discovery, else keep it enable with multi nodes

# Prevent the "split brain" by configuring the majority of nodes (total number of nodes / 2 + 1):

#discovery.zen.minimum\_master\_nodes: 2

# If only one node in the cluster, disable above discovery, else keep it enable with multi nodes

# For more information, see the documentation at:

#http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-discovery.html>

# ---------------------------------- Gateway -----------------------------------

# Block initial recovery after a full cluster restart until N nodes are started:

#gateway.recover\_after\_nodes: 3

# For more information, see the documentation at:

#<http://www.elastic.co/guide/en/elasticsearch/reference/current/modules-gateway.html>

# ---------------------------------- Various -----------------------------------

# Disable starting multiple nodes on a single system:

node.max\_local\_storage\_nodes: 1

#If only one node in the cluster, enable this setting, else keep it disabled

# Require explicit names when deleting indices:

action.destructive\_requires\_name: true

#If only one node in the cluster, enable this setting, else keep it disabled

## ---------------------------------- X-Pack -----------------------------------

#Set to false to disable X-Pack security. Configure in bothelasticsearch.yml and kibana.yml

xpack.security.enabled: true

#Set to false to disable X-Pack monitoring. Configure in bothelasticsearch.yml and kibana.yml

xpack.monitoring.enabled: true

#Set to false to disable X-Pack graph. Configure in bothelasticsearch.yml and kibana.yml

xpack.graph.enabled: true

#Set to false to disable Watcher. Configure in elasticsearch.yml only

xpack.watcher.enabled: true

#

创建相关文件夹和权限

# mkdir -pv /app/elasticsearch/data

# mkdir -pv /app/elasticsearch/logs

# chown gelcmw.gelcmw /app/elasticsearch -R

### 4.3.2 配置/app/elasticsearch/config/log4j2.properties

保持默认配置。

以下是官网介绍

Elasticsearch uses [Log4j 2](http://logging.apache.org/log4j/2.x/) for logging. Log4j 2 can be configured using the log4j2.properties file. Elasticsearch exposes a single property ${sys:es.logs} that can be referenced in the configuration file to determine the location of the log files; this will resolve to a prefix for the Elasticsearch log file at runtime.

For example, if your log directory (path.logs) is /var/log/elasticsearch and your cluster is namedproduction then ${sys:es.logs} will resolve to /var/log/elasticsearch/production.

appender.rolling.type = RollingFile https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/1.png

appender.rolling.name = rolling

appender.rolling.fileName = ${sys:es.logs}.log https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/2.png

appender.rolling.layout.type = PatternLayout

appender.rolling.layout.pattern = [%d{ISO8601}][%-5p][%-25c] %.10000m%n

appender.rolling.filePattern = ${sys:es.logs}-%d{yyyy-MM-dd}.log https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/3.png

appender.rolling.policies.type = Policies

appender.rolling.policies.time.type = TimeBasedTriggeringPolicy https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/4.png

appender.rolling.policies.time.interval = 1 https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/5.png

appender.rolling.policies.time.modulate = true https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/6.png

|  |  |
| --- | --- |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/1.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-1) | Configure the RollingFile appender |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/2.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-2) | Log to /var/log/elasticsearch/production.log |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/3.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-3) | Roll logs to /var/log/elasticsearch/production-yyyy-MM-dd.log |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/4.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-4) | Using a time-based roll policy |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/5.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-5) | Roll logs on a daily basis |
| [https://www.elastic.co/guide/en/elasticsearch/reference/5.0/images/icons/callouts/6.png](https://www.elastic.co/guide/en/elasticsearch/reference/5.0/settings.html#CO6-6) | Align rolls on the day boundary (as opposed to rolling every twenty-four hours) |

### 4.3.3 配置/app/elasticsearch/config/jvm.options

By default, Elasticsearch tells the JVM to use a heap with a minimum and maximum size of 2 GB.

The more heap available to Elasticsearch, the more memory it can use for caching.

But note that too much heap can subject you to long garbage collection pauses.

Set Xmx to no more than 50% of your physical RAM, to ensure that there is enough physical RAM left for kernel file system caches.

# vi /app/elasticsearch/config/jvm.options

## JVM configuration###########################################################

## IMPORTANT: JVM heap size###########################################

## You should always set the min and max JVM heap

## size to the same value. For example, to set

## the heap to 4 GB, set:

## -Xms4g

## -Xmx4g

## See https://www.elastic.co/guide/en/elasticsearch/reference/current/heap-size.html

## for more informatio#########################################################

# Xms represents the initial size of total heap space

# Xmx represents the maximum size of total heap space

-Xms8g

-Xmx8g

### 4.3.4 其他系统配置

#### 4.3.4.1设置最大文件打开数

通过/etc/security/limits.conf 设置永久最大用户打开文件数

. To set the maximum number of open files for the elasticsearch user to 65,536,

add the following line to the limits.conf file:

vi /etc/security/limits.conf

\* hard nofile 131073

\* soft nofile 65536

\* soft nproc 2048

\* hard nproc 4096

gelcmw soft memlock unlimited

gelcmw hard memlock unlimited

#### 4.3.4.2设置virtual memory

# vi /etc/sysctl.conf

# System default settings live in /usr/lib/sysctl.d/00-system.conf.

# To override those settings, enter new settings here, or in an /etc/sysctl.d/<name>.conf file

# For more information, see sysctl.conf(5) and sysctl.d(5).

vm.swappiness = 0

**vm.max\_map\_count=262144**

重启后生效

# sysctl -a|grep vm.max\_map\_count

vm.max\_map\_count = 262144

## 4.4 配置elasticsearch服务启动

### 4.4.1 手动启动elasticsearch服务

通过非root用户(gelcmw)以守护进程启动elasticsearch

#/app/elasticsearch/bin/elasticsearch -d

检查elasticsearch是否启动

# lsof -i :9200

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

java 8834 gelcmw 129u IPv6 30605 0t0 TCP localhost:wap-wsp (LISTEN)

java 8834 gelcmw 130u IPv6 30606 0t0 TCP localhost:wap-wsp (LISTEN)

# curl 10.163.36.22:9200

{

"name" : "D2-ELK22",

"cluster\_name" : "elk\_cluster",

"cluster\_uuid" : "\_na\_",

"version" : {

"number" : "5.0.0",

"build\_hash" : "253032b",

"build\_date" : "2016-10-26T04:37:51.531Z",

"build\_snapshot" : false,

"lucene\_version" : "6.2.0"

},

"tagline" : "You Know, for Search"

Website : <http://10.163.36.22:9200>



关闭elasticsearch

# lsof -i :9200

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

java 8834 gelcmw 129u IPv6 30605 0t0 TCP localhost:wap-wsp (LISTEN)

java 8834 gelcmw 130u IPv6 30606 0t0 TCP localhost:wap-wsp (LISTEN)

# **kill 8834**

# 5 安装Logstash

在D2-ELK21安装Logstash

Logstash v5.0.0 下载地址

<https://www.elastic.co/downloads/logstash>

## 5.1 安装tar.gz包

mv logstash-5.0.1.tar.gz /app/

tar zxvf logstash-5.0.1.tar.gz

mv /app/logstash-5.0.1 /app/logstash

tar.gz安装的文件目录如下

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Description | Default Location | Setting |
| home | Home directory of the Logstash installation | /app/logstash |  |
| bin | Binary scripts, including logstash to start Logstash and logstash-plugin to install plugins | /app/logstash /bin |  |
| settings | Configuration files, including logstash.yml and jvm.options | /app/logstash /config | path.settings |
| logs | Log files location. | /app/logstash /logs | path.logs |
| plugins | Local, non Ruby-Gem plugin files. Each plugin is contained in a subdirectory. Recommended for development only. | /app/logstash /plugins |  |

## 5.2 设置Logstash配置文件

### 5.2.1 配置/app/logstash/config/logstash.yml

Logstash的默认配置文件在 /app/logstash/config/logstash.yml

The format of this config file is explained in

https://www.elastic.co/guide/en/logstash/current/logstash-settings-file.html

# vi /app/logstash/config/logstash.yml

# Settings file in YAML

# Settings can be specified either in hierarchical form, e.g.:

# pipeline:

# batch:

# size: 125

# delay: 5

#

# Or as flat keys:

## pipeline.batch.size: 125

# pipeline.batch.delay: 5

# ------------ Node identity ------------

# Use a descriptive name for the node:

node.name: **10.163.36.123-D2-CJYTEST123**

# If omitted the node name will default to the machine's host name

# ------------ Data path ------------------

# Which directory should be used by logstash and its plugins

# for any persistent needs. Defaults to LOGSTASH\_HOME/data

# path.data:

# ------------ Pipeline Settings --------------

# Set the number of workers that will, in parallel, execute the filters+outputs

# stage of the pipeline.

# This defaults to the number of the host's CPU cores.

pipeline.workers: 2

# How many workers should be used per output plugin instance

pipeline.output.workers: 1

# How many events to retrieve from inputs before sending to filters+workers

pipeline.batch.size: 125

# How long to wait before dispatching an undersized batch to filters+workers

# Value is in milliseconds.

pipeline.batch.delay: 5

# Force Logstash to exit during shutdown even if there are still inflight

# events in memory. By default, logstash will refuse to quit until all

# received events have been pushed to the outputs.

# WARNING: enabling this can lead to data loss during shutdown

pipeline.unsafe\_shutdown: false

# ------------ Pipeline Configuration Settings --------------

# Where to fetch the pipeline configuration for the main pipeline

path.config: /app/logstash/config/conf

# Pipeline configuration string for the main pipeline

# config.string:

# At startup, test if the configuration is valid and exit (dry run)

config.test\_and\_exit: false

# Periodically check if the configuration has changed and reload the pipeline

# This can also be triggered manually through the SIGHUP signal

config.reload.automatic: false

# How often to check if the pipeline configuration has changed (in seconds)

# config.reload.interval: 3

# Show fully compiled configuration as debug log message

# NOTE: --log.level must be 'debug'

# config.debug: false

# ------------ Metrics Settings --------------

# Bind address for the metrics REST endpoint

http.host: "10.163.36.123"

# Bind port for the metrics REST endpoint, this option also accept a range

# (9600-9700) and logstash will pick up the first available ports.

http.port: 9600-9700

# ------------ Debugging Settings --------------

# Options for log.level:

# \* fatal

# \* error

# \* warn

# \* info (default)

# \* debug

# \* trace

#

log.level: info

path.logs: /app/logstash/logs

# ------------ Other Settings --------------

# Where to find custom plugins

# path.plugins: []

### 5.2.2 测试logstash日志传送

#### 5.2.2.1日志本地传送

$ /app/logstash/bin/logstash -e 'input { stdin { } } output { stdout {} }'

hello

Sending Logstash's logs to /app/logstash/logs which is now configured via log4j2.properties

[2016-11-16T17:34:43,760][INFO ][logstash.agent ] Successfully started Logstash API endpoint {:port=>9600}

2016-11-16T09:34:43.719Z D2-ELK21 hello

#### 5.2.2.2日志传送到elasticsearch

配置logstash config

# cat /app/logstash/config/logstash\_test.conf

input {

stdin { }

}

output {

elasticsearch {hosts => "10.163.36.22" }

stdout { codec=> rubydebug }

}

测试logstash 传送日志到elasticsearch

# /app/logstash/bin/logstash -f /app/logstash/config/logstash\_test.conf

Sending Logstash's logs to /app/logstash/logs which is now configured via log4j2.properties

[2016-11-17T10:33:57,017][INFO ][logstash.agent ] Successfully started Logstash API endpoint {:port=>9600}

hello Ethan chen

{ "@timestamp" => 2016-11-17T02:41:28.896Z,

"@version" => "1",

"host" => "D2-ELK21",

"message" => "hello Ethan chen",

"tags" => []}

查看logstash 传送日志到elasticsearch

<http://10.163.36.22:9200/_search?pretty>

或者

# curl 'http://10.163.36.22:9200/\_search?pretty'

{

"\_index" : "logstash-2016.11.17",

"\_type" : "logs",

"\_id" : "AVhwKRHVwbpaleMcmZ\_p",

"\_score" : 1.0,

"\_source" : {

"@timestamp" : "2016-11-17T02:41:28.896Z",

"@version" : "1",

"host" : "D2-ELK21",

"message" : "hello Ethan chen",

"tags" : [ ]

}

},

## 5.3 配置jvm.options

Logstash默认会使用256M -1G 内存heap space.

可以按实际环境调整。

# vi /app/logstash/config/jvm.options

# JVM configuration

# Xms represents the initial size of total heap space

# Xmx represents the maximum size of total heap space

-Xms256m

-Xmx1g

## 5.4客户端系统的logstash conf配置样例

参考官方样例

<https://www.elastic.co/guide/en/logstash/current/config-examples.html>

<https://www.elastic.co/guide/en/logstash/current/configuration-file-structure.html>

<http://kibana.logstash.es/content/logstash/get_start/full_config.html>

http://kibana.logstash.es/content/logstash/examples/

### 5.4.1配置本地系统日志传送

本范例主要是索引本地系统日志

#cat /app/logstash/config/syslog.conf

input {

file {

type => "syslog"

path => ["/var/log/messages", "/var/log/secure" ]

exclude => ["\*.gz"]

}

syslog {

type => "syslog"

port => "5544"

}

}

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}" ]

}

date {

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

}

}

}

output {

elasticsearch {

hosts => ["10.163.36.22" ]

user => "elastic"

password => ",ki89ol."

index => "syslog-%{+YYYY.MM.dd.HH}" --自定义index名称，需要与kibana创建索引时一致

}

}

### 5.4.2配置apache 日志传送

Apache日志：自定义apache输出日志格式，json输出，无需filter参与

将apache httpd的access日志output到elasticsearch上，并通过kibana显示日志

vim /app/logstash/config/logstash-apache.conf

input {

file {

path => "/var/log/httpd/access\_log"

codec => "json"

}

}

filter {

if [path] =~ "access" {

mutate { replace => { "type" => "apache\_access" } }

grok {

match => { "message" => "%{COMBINEDAPACHELOG}" }

}

}

date {

match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]

}

}

output {

elasticsearch {

hosts => ["10.163.36.22:9200"] --ELK服务端ip地址和端口

user => "elastic"

password => ",ki89ol."

index => "apache-log-%{+YYYY.MM.dd.HH}" --index名称，自定义的

template\_overwrite => true

}

}

### 5.4.3配置Tomcat catalina.out 日志传送

Tomcat日志：需将多行日志合并至一个事件中，并排除空白行

vim /app/logstash/config/tomcat.conf

input {

file {

type => "tomcat"

path => [ "/app/tomcat/apache-tomcat-8.5.5/logs/catalina.out" ]

codec => multiline {

pattern => "(^\d+\serror)|(^.+Exception:.+)|(^\s+at .+)|(^\s+... \d+ more)|(^\s\*Caused by:.+)"

what => "previous"

}

}

}

filter {

if [type] == "tomcat" and "multiline" in [tags]{

grok {

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

}

}

}

output{

elasticsearch{

hosts => ["10.163.36.22:9200"]

user => "elastic"

password => ",ki89ol."

index => "tomcat-%{+YYYY.MM.dd.HH}"

template\_overwrite => true

}

}

## 5.5 设置客户端系统的logstash服务长期运行

通过nohup & 方式,使logstash长期后台运行

#

**nohup** /app/logstash/bin/logstash -f /app/logstash/config/conf/logstash-http.conf **&**

如果执行多个conf文件如下

#

**nohup** /app/logstash/bin/logstash -f /app/logstash/config/conf/\*.conf **&**

具体说明参考以下链接

http://kibana.logstash.es/content/logstash/get\_start/daemon.html

# 6 安装kibana

在D2-ELK21安装kibana

kibana v5.0.0 下载地址

https://www.elastic.co/downloads/kibana

## 6.1 安装tar.gz包

mv kibana-5.0.1.tar.gz /app/

tar zxvf kibana-5.0.1.tar.gz

mv /app/ kibana-5.0.1 /app/ kibana

tar.gz安装的文件目录如下

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Description | Default Location | Setting |
| home | Kibana home directory or $KIBANA\_HOME | /app/kibana |  |
| bin | Binary scripts including kibana to start the Kibana server and kibana-plugin to install plugins | /app/kibana /bin |  |
| config | Configuration files including kibana.yml | /app/kibana /config |  |
| data | The location of the data files written to disk by Kibana and its plugins | /app/kibana /data |  |
| optimize | Transpiled source code. Certain administrative actions (e.g. plugin install) result in the source code being retranspiled on the fly. | /app/kibana /optimize |  |
| plugins | Plugin files location. Each plugin will be contained in a subdirectory. | //app/kibana /plugins |  |

## 6.2 安装配置X-Pack

### 6.2.1手动下载X-Pack

<https://artifacts.elastic.co/downloads/packs/x-pack/x-pack-5.0.1.zip>

### 6.2.2为Kibana手动安装X-Pack

关闭kibana服务后，在每一个节点的kibana的安装目录下运行 /app/kibana/bin/kibana-plugin 安装X-Pack

# /app/kibana/bin/kibana-plugin install file:///home/gelcmw/x-pack-5.0.1.zip

Attempting to transfer from file:///home/gelcmw/x-pack-5.0.1.zip

Transferring 72393860 bytes....................

Transfer complete

Retrieving metadata from plugin archive

Extracting plugin archive

Extraction complete

Optimizing and caching browser bundles...

Plugin installation complete

### 6.2.3启动X-Pack相关features

X-Pack相关features默认是启动的。

Elasticsearch通过elasticsearch.yml, kibana通过 kibana.yml启动、关闭X-Pack相关features

|  |  |
| --- | --- |
| Setting | Description |
| xpack.security.enabled | Set to false to disable X-Pack security. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.monitoring.enabled | Set to false to disable X-Pack monitoring. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.graph.enabled | Set to false to disable X-Pack graph. Configure in bothelasticsearch.yml and kibana.yml. |
| xpack.watcher.enabled | Set to false to disable Watcher. Configure in elasticsearch.yml only. |
| xpack.reporting.enabled | Set to false to disable X-Pack reporting. Configure in kibana.yml only. |

## 6.3 配置/app/kibana/config/kibana.yml

Kibana的默认配置文件在 /app/kibana/config/kibana.yml

https://www.elastic.co/guide/en/kibana/current/settings.html.

vi /app/kibana/config/kibana.yml # Kibana is served by a back end server. This setting specifies the port to use.

server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.

# The default is 'localhost', which means remote machines will not be able to connect.

# To allow connections from remote users, set this parameter to a non-loopback address.

server.host: "10.163.36.21"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This only affects

# the URLs generated by Kibana, your proxy is expected to remove the basePath value before forwarding requests

# to Kibana. This setting cannot end in a slash.

#server.basePath: ""

# The maximum payload size in bytes for incoming server requests.

server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.

server.name: "D2-ELK21-Kibana"

# The URL of the Elasticsearch instance to use for all your queries.

elasticsearch.url: "http://10.163.36.22:9200"

# When this setting’s value is true Kibana uses the hostname specified in the server.host

# setting. When the value of this setting is false, Kibana uses the hostname of the host

# that connects to this Kibana instance.

elasticsearch.preserveHost: false

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and

# dashboards. Kibana creates a new index if the index doesn’t already exist.

kibana.index: ".kibana"

# The default application to load.

kibana.defaultAppId: "discover"

# If your Elasticsearch is protected with basic authentication, these settings provide

# the username and password that the Kibana server uses to perform maintenance on the Kibana

# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which

# is proxied through the Kibana server.

elasticsearch.username: "elastic"

elasticsearch.password: "changeme"

# Paths to the PEM-format SSL certificate and SSL key files, respectively. These

# files enable SSL for outgoing requests from the Kibana server to the browser.

#server.ssl.cert: /path/to/your/server.crt

#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.

# These files validate that your Elasticsearch backend uses the same key files.

#elasticsearch.ssl.cert: /path/to/your/client.crt

#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the certificate

# authority for your Elasticsearch instance.

#elasticsearch.ssl.ca: /path/to/your/CA.pem

# To disregard the validity of SSL certificates, change this setting’s value to false.

#elasticsearch.ssl.verify: true

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of

# the elasticsearch.requestTimeout setting.

elasticsearch.pingTimeout: 1500

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value

# must be a positive integer.

elasticsearch.requestTimeout: 30000

# List of Kibana client-side headers to send to Elasticsearch. To send \*no\* client-side

# headers, set this value to [] (an empty list).

#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom headers cannot be overwritten

# by client-side headers, regardless of the elasticsearch.requestHeadersWhitelist configuration.

#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.

#elasticsearch.shardTimeout: 0

# Time in milliseconds to wait for Elasticsearch at Kibana startup before retrying.

elasticsearch.startupTimeout: 5000

# Specifies the path where Kibana creates the process ID file.

pid.file: /app/kibana/kibana.pid

# Enables you specify a file where Kibana stores log output.

logging.dest: stdout

# Set the value of this setting to true to suppress all logging output.

logging.silent: true

# Set the value of this setting to true to suppress all logging output other than error messages.

logging.quiet: true

# Set the value of this setting to true to log all events, including system usage information

# and all requests.

#logging.verbose: false

# Set the interval in milliseconds to sample system and process performance

# metrics. Minimum is 100ms. Defaults to 5000.

ops.interval: 5000

# ---------------------------------- X-Pack -----------------------------------

#Set to false to disable X-Pack security. Configure in bothelasticsearch.yml and kibana.yml

xpack.security.enabled: true

#Set to false to disable X-Pack monitoring. Configure in bothelasticsearch.yml and kibana.yml

xpack.monitoring.enabled: true

#Set to false to disable X-Pack graph. Configure in bothelasticsearch.yml and kibana.yml

xpack.graph.enabled: true

#Set to false to disable X-Pack reporting. Configure in kibana.yml only

xpack.reporting.enabled: true

## 6.4 配置kibana服务启动

### 6.4.1 手动启动kibana服务

后台启动kibana

#/app/kibana/bin/kibana -d

检查kibana是否启动

# lsof -i :5601

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

node 20802 gelcmw 12u IPv4 335794 0t0 TCP D2-ELK21:esmagent (LISTEN)

# curl 10.163.36.22:9200

{

"name" : "D2-ELK22",

"cluster\_name" : "elk\_cluster",

"cluster\_uuid" : "\_na\_",

"version" : {

"number" : "5.0.0",

"build\_hash" : "253032b",

"build\_date" : "2016-10-26T04:37:51.531Z",

"build\_snapshot" : false,

"lucene\_version" : "6.2.0"

},

"tagline" : "You Know, for Search"

Website : <http://10.163.36.22:9200>



关闭elasticsearch

# lsof -i :9200

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

java 8834 gelcmw 129u IPv6 30605 0t0 TCP localhost:wap-wsp (LISTEN)

java 8834 gelcmw 130u IPv6 30606 0t0 TCP localhost:wap-wsp (LISTEN)

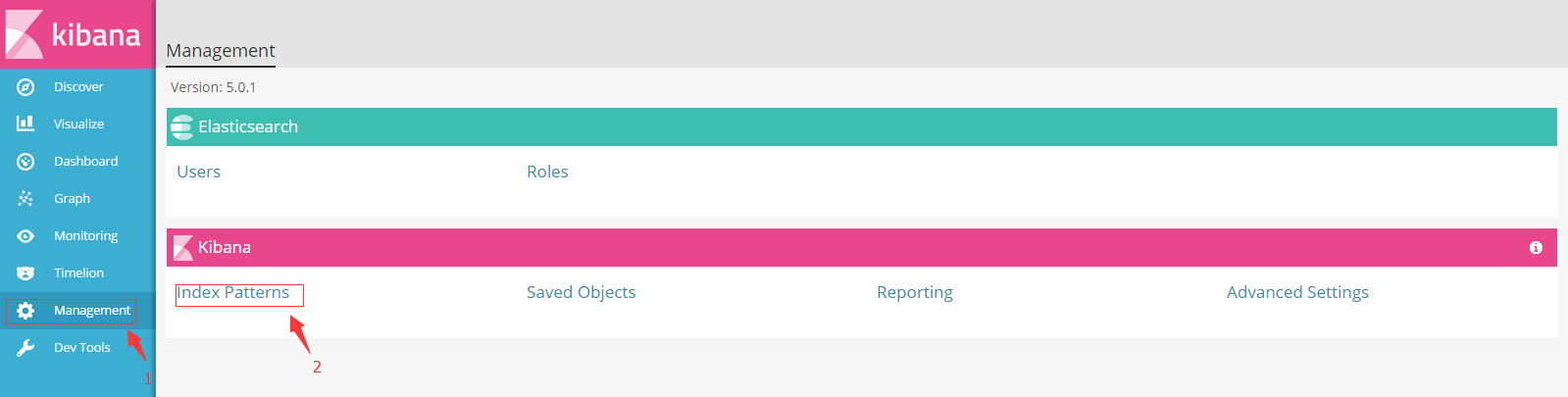
# **kill 8834**

## 6.5 配置kibana 日志索引

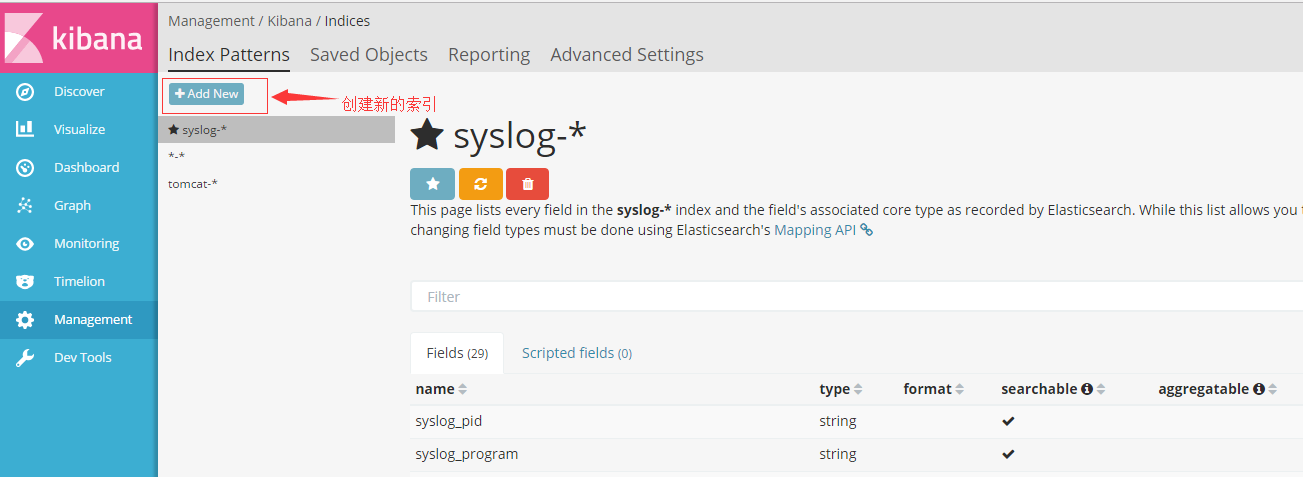
### 6.5.1创建索引

以5.4.1本地系统日志传送在kibana界面创建一个新的index

点击“Management”,选择 “Index Patterns“

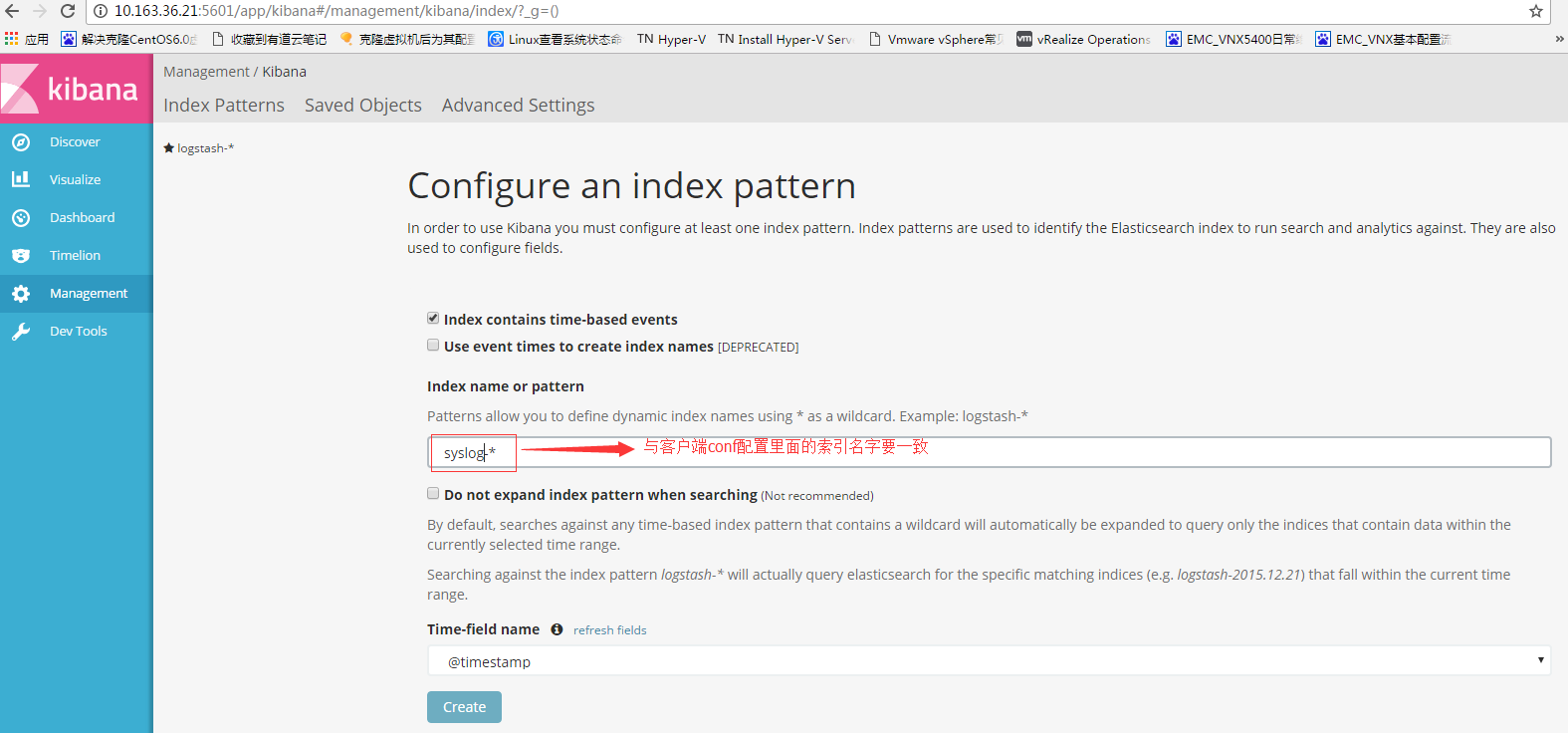


点击“ Add New” 创建新索引

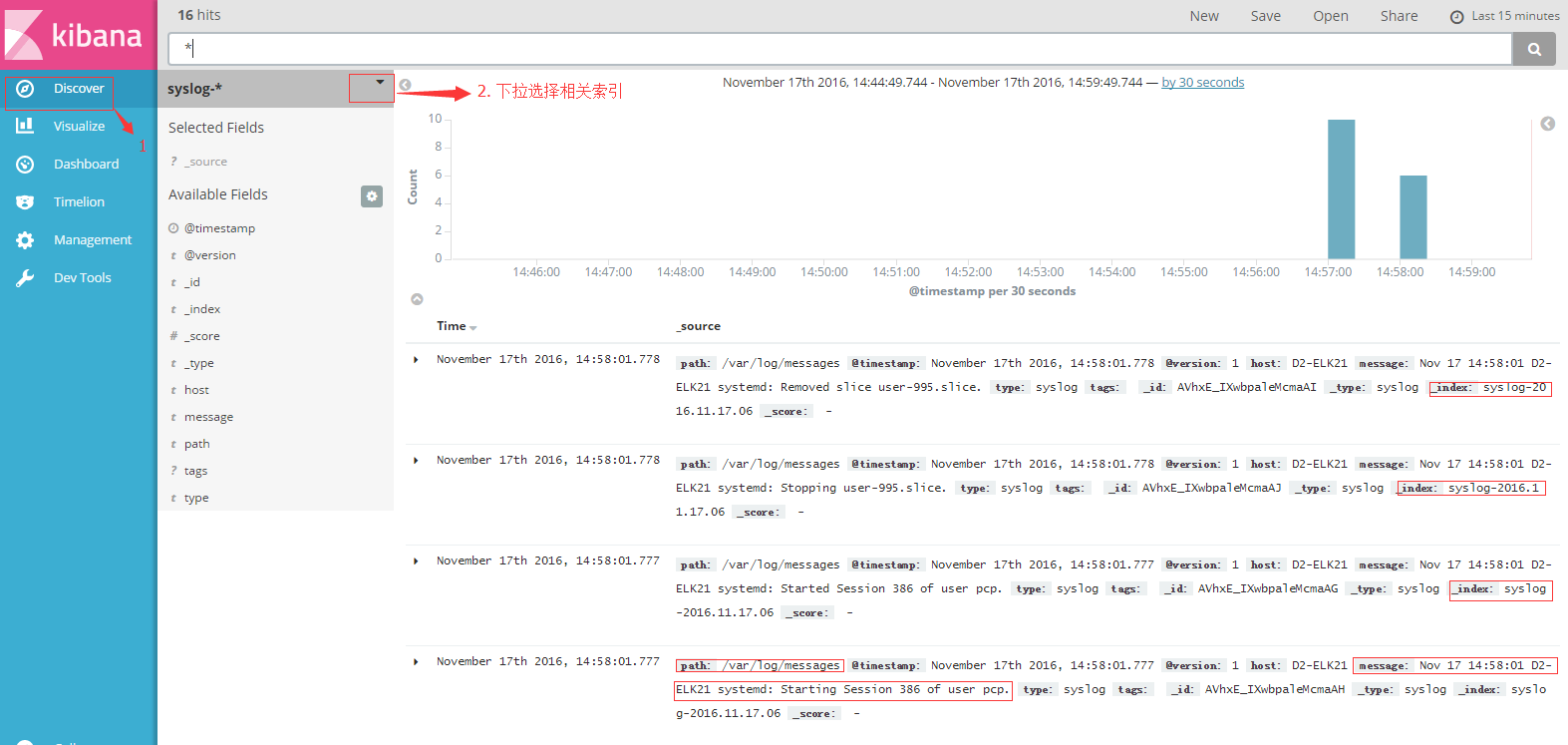


填写如下内容 syslog-\*

（此内容必须如logstash客户端配置文件里面的索引名字一致）



在”Discovery” 下拉选择syslog-\* ，查看相关系统日志

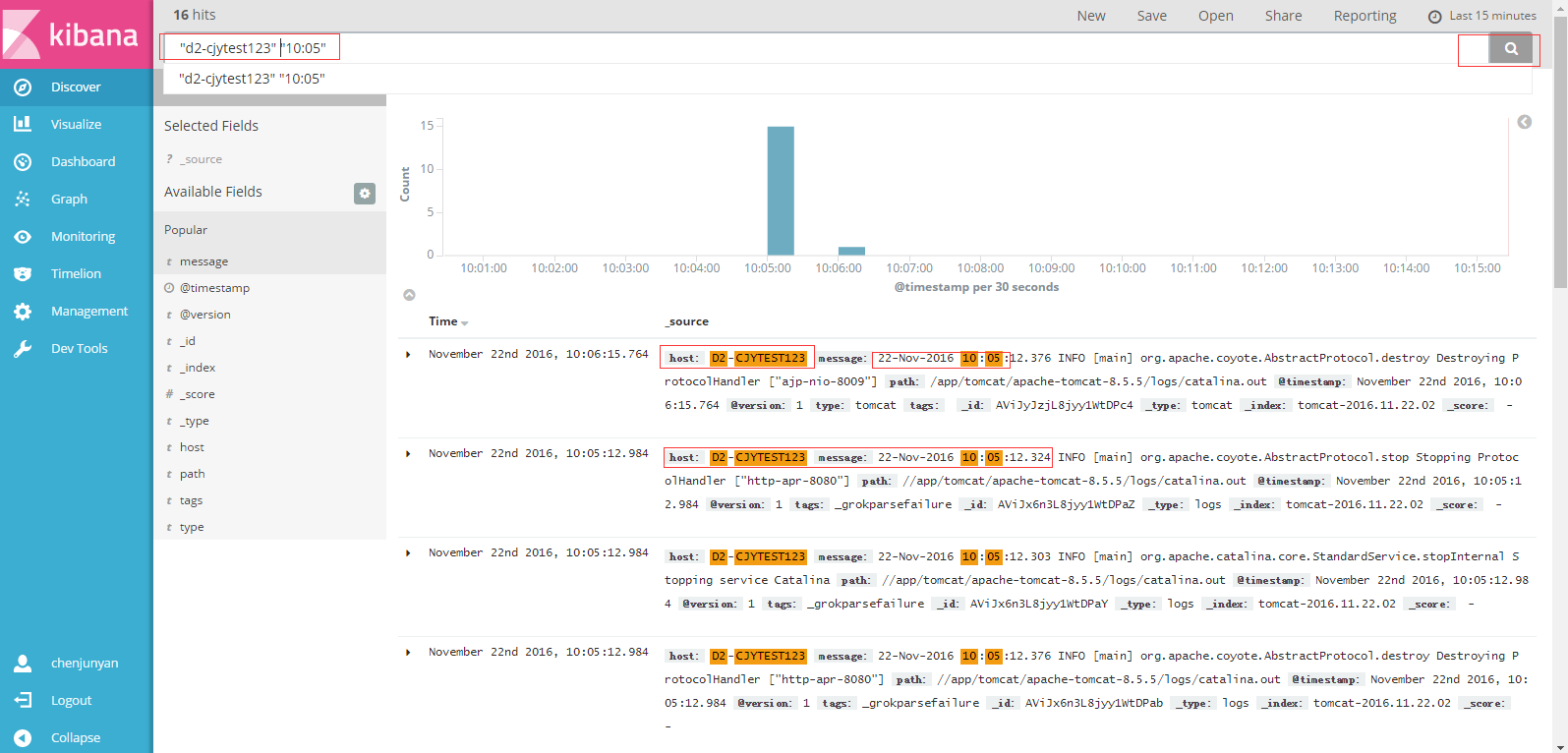


### 6.5.2 搜索相关日志

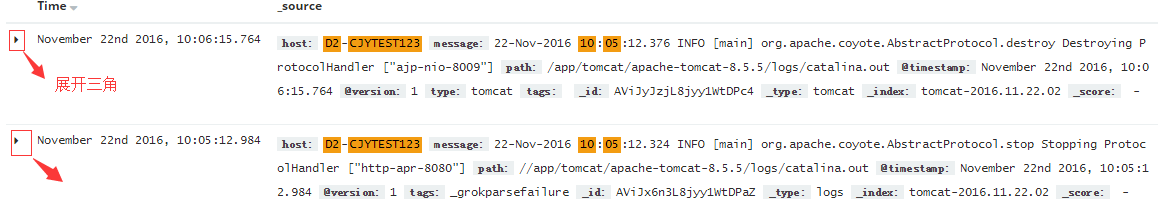
在搜索框，输入相关内容，类如主机名或者日志时间（需要双引号定义范围）

"d2-cjytest123" "10:05"

点击搜索后，相关内容就会如下图显示



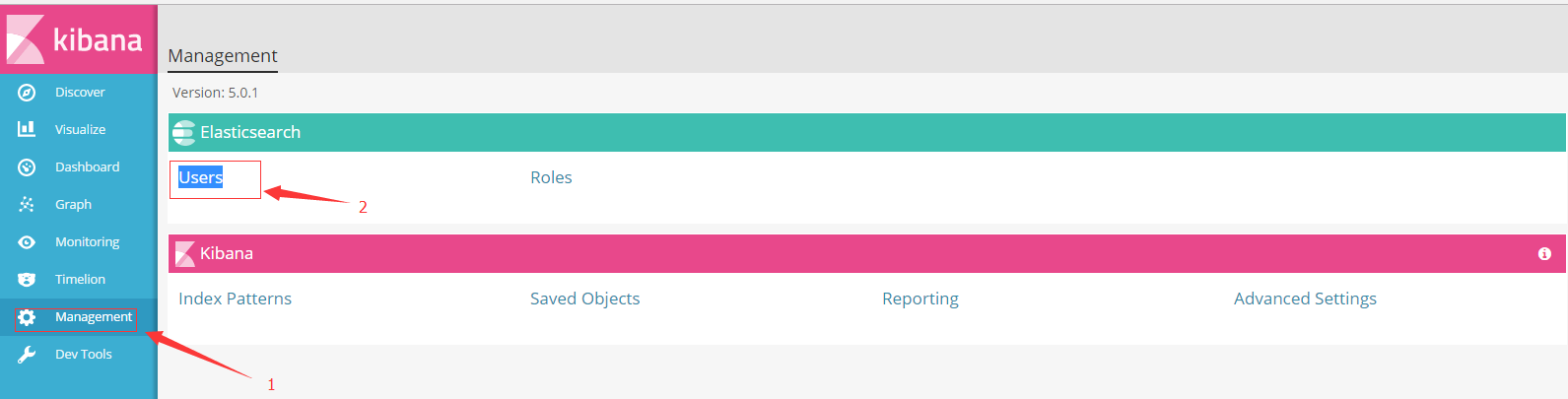
在想要看的日志，点击展示三角符号，查看详细信息





### 6.5.3 创建kibana用户

点击“Management”,选择 “User“



一般选择”supperuser” 角色

