实验四 基于Docker搭建ELK

实验文档参考地址：
https://developer.aliyun.com/adc/scenario/fe0284e0e2fe4817923a468ba5b4fa0a

1. 检查Docker环境

检查docker是否安装，如没有安装，可根据前面的实验一步骤安装Docker环境。

Plain Text

```
docker version
```

```
[root@ELK ~]# docker version
Client: Docker Engine - Community
 Version:           20.10.6
 API version:       1.41
 Go version:        go1.13.15
 Git commit:        370c289
 Built:             Fri Apr  9 22:44:36 2021
 OS/Arch:           linux/amd64
 Context:           default
 Experimental:      true

Server: Docker Engine - Community
 Engine:
  Version:          20.10.6
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.13.15
  Git commit:       8728dd2
  Built:            Fri Apr  9 22:43:02 2021
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.4.6
  GitCommit:        d71fcd7d8303cbf684402823e425e9dd2e99285d
 runc:
  Version:          1.0.0-rc95
  GitCommit:        b9ee9c6314599f1b4a7f497e1f1f856fe433d3b7
 docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0
[root@ELK ~]#
```

```
[root@ELK ~]# cat /etc/docker/daemon.json
{
"registry-mirrors": ["https://e7n1ndig.mirror.aliyuncs.com"]
}
[root@ELK ~]#
```

Plain Text

```
# cat /etc/docker/daemon.json
```

2. 下载实验需要的镜像

Plain Text

```
docker pull elasticsearch
```

```
[root@ELK ~]# docker images
REPOSITORY      TAG       IMAGE ID       CREATED       SIZE
nginx           latest    4f380adfc10f   4 days ago    133MB
logstash        latest    33c2b80b5322   2 years ago   653MB
kibana          latest    a674d23325b0   2 years ago   388MB
elasticsearch   latest    5acf0e8da90b   2 years ago   486MB
[root@ELK ~]#
```

Plain Text

```
docker pull kibana
```

Plain Text

```
docker pull logstash
```

Plain Text

```
docker pull nginx
```

Plain Text

```
docker images
```

3. 部署Elasticsearch

a. 修改JVM堆大小

默认情况下，Elasticsearch的JVM使用的堆大小为2GB，可以修改ES的jvm默认参数

Plain Text

```
find /var/lib/docker/overlay2/ -name jvm.options
```

```
[root@ELK ~]# find /var/lib/docker/overlay2/ -name jvm.options
/var/lib/docker/overlay2/e1d875c1bca936d5d10b03721de3c83081e815fc7db9c9be814e54878db31a90/diff/etc/elasticsearch/jvm.options
[root@ELK ~]#
```

修改相应的配置文件

–Xms2g 改为 –Xms1g

–Xmx2g 改为 –Xmx1g

```
#################################################################

# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

-Xms1g
-Xmx1g
```

b. 调整vm.max_map_count大小

Plain Text

```
vim /etc/sysctl.conf
```

```
vm.swappiness = 0
kernel.sysrq = 1

net.ipv4.neigh.default.gc_stale_time = 120

# see details in https://help.aliyun.com/knowledge_detail/39428.html
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.arp_announce = 2
net.ipv4.conf.lo.arp_announce = 2
net.ipv4.conf.all.arp_announce = 2

# see details in https://help.aliyun.com/knowledge_detail/41334.html
net.ipv4.tcp_max_tw_buckets = 5000
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.tcp_synack_retries = 2

vm.max_map_count=262144
~
~
```

Plain Text

```
sysctl -p
```

```
[root@ELK ~]# sysctl -p
vm.swappiness = 0
kernel.sysrq = 1
net.ipv4.neigh.default.gc_stale_time = 120
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.default.arp_announce = 2
net.ipv4.conf.lo.arp_announce = 2
net.ipv4.conf.all.arp_announce = 2
net.ipv4.tcp_max_tw_buckets = 5000
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.tcp_synack_retries = 2
vm.max_map_count = 262144
[root@ELK ~]#
```

c. 启动elasticsearch容器

Plain Text

```
docker run --name elasticsearch -v "$PWD/esdata":/usr/share/elasticsearch/data -p 9200:9200 -d elasticsearch
```

```
[root@ELK ~]# docker run --name elasticsearch -v "$PWD/esdata":/usr/share/elasticsearch/data -p 9200:9200 -d elasticsearch
bf100ae8fd6de37fda9b9289f319abb8cf4ce2246bb18d45b7b580a6e17a7d10
[root@ELK ~]#
```

Plain Text

```
docker logs elasticsearch
```

```
[root@ELK ~]# docker logs elasticsearch
[2021-06-28T12:43:28,684][INFO ][o.e.n.Node               ] [] initializing ...
[2021-06-28T12:43:28,744][INFO ][o.e.e.NodeEnvironment    ] [Ds4s2jF] using [1] data paths, mounts [[/usr/share/elasticsearch/data (/dev/vda1)]], net usable_space [3
5.7gb], net total_space [39.9gb], spins? [possibly], types [xfs]
[2021-06-28T12:43:28,744][INFO ][o.e.e.NodeEnvironment    ] [Ds4s2jF] heap size [1007.3mb], compressed ordinary object pointers [true]
[2021-06-28T12:43:28,745][INFO ][o.e.n.Node               ] node name [Ds4s2jF] derived from node ID [Ds4s2jFJQom_gQMdk5O1GA]; set [node.name] to override
[2021-06-28T12:43:28,746][INFO ][o.e.n.Node               ] version[5.6.12], pid[1], build[cfe3d9f/2018-09-10T20:12:43.732Z], OS[Linux/4.18.0-193.28.1.el8_2.x86_64/a
md64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/1.8.0_181/25.181-b13]
[2021-06-28T12:43:28,746][INFO ][o.e.n.Node               ] JVM arguments [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:+UseCM
SInitiatingOccupancyOnly, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -Djdk.io.permissionsUseCanonicalPath=true,
-Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=t
rue, -Dlog4j.skipJansi=true, -XX:+HeapDumpOnOutOfMemoryError, -Des.path.home=/usr/share/elasticsearch]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [aggs-matrix-stats]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [ingest-common]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [lang-expression]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [lang-groovy]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [lang-mustache]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [lang-painless]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [parent-join]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [percolator]
[2021-06-28T12:43:29,372][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [reindex]
[2021-06-28T12:43:29,373][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [transport-netty3]
[2021-06-28T12:43:29,373][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] loaded module [transport-netty4]
[2021-06-28T12:43:29,376][INFO ][o.e.p.PluginsService     ] [Ds4s2jF] no plugins loaded
[2021-06-28T12:43:30,793][INFO ][o.e.d.DiscoveryModule    ] [Ds4s2jF] using discovery type [zen]
[2021-06-28T12:43:31,180][INFO ][o.e.n.Node               ] initialized
[2021-06-28T12:43:31,181][INFO ][o.e.n.Node               ] [Ds4s2jF] starting ...
[2021-06-28T12:43:31,200][INFO ][o.e.t.TransportService   ] [Ds4s2jF] publish_address {127.0.0.1:9300}, bound_addresses {127.0.0.1:9300}
[2021-06-28T12:43:31,267][WARN ][o.e.b.BootstrapChecks    ] [Ds4s2jF] max virtual memory areas vm.max_map_count [65530] is too low, increase to at least [262144]
[2021-06-28T12:43:34,362][INFO ][o.e.c.s.ClusterService   ] [Ds4s2jF] new_master {Ds4s2jF}{Ds4s2jFJQom_gQMdk5O1GA}{s6U2MMHr5PeJXohLaWRrHA}{127.0.0.1}{127.0.0.1:9300}
, reason: zen-disco-elected-as-master ([0] nodes joined)[, ]
[2021-06-28T12:43:34,370][INFO ][o.e.h.n.Netty4HttpServerTransport] [Ds4s2jF] publish_address {172.18.0.2:9200}, bound_addresses {0.0.0.0:9200}
[2021-06-28T12:43:34,370][INFO ][o.e.n.Node               ] [Ds4s2jF] started
[2021-06-28T12:43:34,383][INFO ][o.e.g.GatewayService     ] [Ds4s2jF] recovered [0] indices into cluster_state
[root@ELK ~]#
```

Plain Text

```
curl http://localhost:9200
```

```
[root@ELK ~]# curl http://localhost:9200
{
  "name" : "Ds4s2jF",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "B2hq5v1wSdmCLBHvN-dbhw",
  "version" : {
    "number" : "5.6.12",
    "build_hash" : "cfe3d9f",
    "build_date" : "2018-09-10T20:12:43.732Z",
    "build_snapshot" : false,
    "lucene_version" : "6.6.1"
  },
  "tagline" : "You Know, for Search"
}
[root@ELK ~]#
```

Plain Text

```
docker run --name logstash --link elasticsearch:elasticsearch -p 5044:5044 -d -v /docker/config/logstash:/config-dir logstash -f /config-dir/logstash.conf
```

```
[root@ELK ~]# docker run --name logstash --link elasticsearch:elasticsearch -p 5044:5044 -d -v /docker/config/logstash:/config-di
r logstash -f /config-dir/logstash.conf
ac7e137477955fbee6c7af9c5a3f313965a9e0fea79041acfccce6894513055f
[root@ELK ~]#
```

Plain Text

```
docker logs logstash
```

```
[root@ELK ~]# docker logs logstash
Sending Logstash's logs to /var/log/logstash which is now configured via log4j2.properties
00:16:22.132 [main] INFO  logstash.modules.scaffold - Initializing module {:module_name=>"fb_apache", :directory=>"/usr/share/logstash/modules/fb_apache/configuratio
n"}
00:16:22.135 [main] INFO  logstash.modules.scaffold - Initializing module {:module_name=>"netflow", :directory=>"/usr/share/logstash/modules/netflow/configuration"}
00:16:22.137 [main] INFO  logstash.setting.writabledirectory - Creating directory {:setting=>"path.queue", :path=>"/var/lib/logstash/queue"}
00:16:22.138 [main] INFO  logstash.setting.writabledirectory - Creating directory {:setting=>"path.dead_letter_queue", :path=>"/var/lib/logstash/dead_letter_queue"}
00:16:22.152 [LogStash::Runner] INFO  logstash.agent - No persistent UUID file found. Generating new UUID {:uuid=>"53101e8f-e128-4c3c-82b6-cfe0d2ebe320", :path=>"/va
r/lib/logstash/uuid"}
00:16:22.453 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[http://elasticsearch
:9200/]}}
00:16:22.455 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Running health check to see if an Elasticsearch connection is working {:healthcheck_url
=>http://elasticsearch:9200/, :path=>"/"}
00:16:22.576 [[main]-pipeline-manager] WARN  logstash.outputs.elasticsearch - Restored connection to ES instance {:url="http://elasticsearch:9200/"}
00:16:22.739 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Using mapping template from {:path=>nil}
00:16:22.741 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Attempting to install template {:manage_template=>{"template"=>"logstash-*", "version"=
>50001, "settings"=>{"index.refresh_interval"=>"5s"}, "mappings"=>{"_default_"=>{"_all"=>{"enabled"=>true, "norms"=>false}, "dynamic_templates"=>[{"message_field"=>{
"path_match"=>"message", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}}, {"string_fields"=>{"match"=>"*", "match_mapping_type"=>"strin
g", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"keyword"=>{"type"=>"keyword", "ignore_above"=>256}}}}}], "properties"=>{"@timestamp"=>{"type"=>"date", "i
nclude_in_all"=>false}, "@version"=>{"type"=>"keyword", "include_in_all"=>false}, "geoip"=>{"dynamic"=>true, "properties"=>{"ip"=>{"type"=>"ip"}, "location"=>{"type"
=>"geo_point"}, "latitude"=>{"type"=>"half_float"}, "longitude"=>{"type"=>"half_float"}}}}}}}}
00:16:22.749 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Installing elasticsearch template to _template/logstash
00:16:22.866 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - New Elasticsearch output {:class=>"LogStash::Outputs::ElasticSearch", :hosts=>["//elast
icsearch:9200"]}
00:16:22.868 [[main]-pipeline-manager] INFO  logstash.pipeline - Starting pipeline {"id"=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.
delay"=>5, "pipeline.max_inflight"=>500}
00:16:23.134 [[main]-pipeline-manager] INFO  logstash.inputs.beats - Beats inputs: Starting input listener {:address=>"0.0.0.0:5044"}
00:16:23.158 [[main]-pipeline-manager] INFO  logstash.pipeline - Pipeline main started
00:16:23.175 [[main]<beats] INFO  org.logstash.beats.Server - Starting server on port: 5044
00:16:23.229 [Api Webserver] INFO  logstash.agent - Successfully started Logstash API endpoint {:port=>9600}
[root@ELK ~]#
```

4. 部署logstash

a. 创建logstash配置文件

```bash
mkdir -p /docker/config/logstash/
```

```plain text
vim /docker/config/logstash/logstash.conf
```

在/docker/config/logstash/目录下创建配置文件logstash.conf，内容如下:

```plain text
input {
     beats {
         port => 5044
         type => beats
     }
}

output {
     elasticsearch {
         hosts => ["elasticsearch:9200"]
     }
}
```

b. 启动logstash容器

```plain text
docker run --name logstash --link elasticsearch:elasticsearch -p 5044:5044 -d -v /docker/config/logstash:/config-dir logstash -f /config-dir/logstash.conf
```

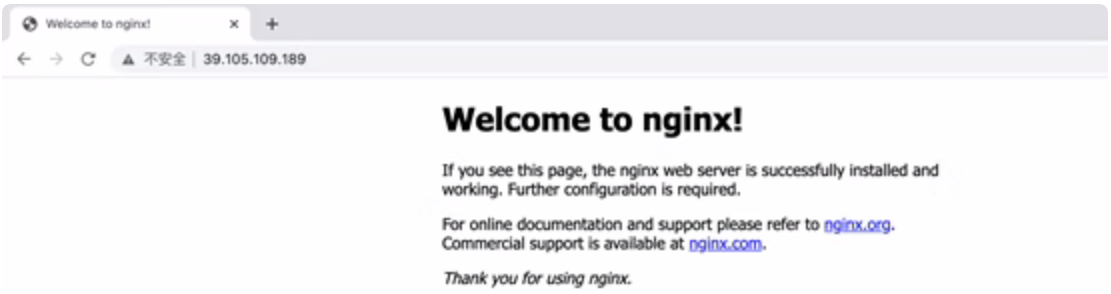
```
[root@ELK ~]# docker run --name logstash --link elasticsearch:elasticsearch -p 5044:5044 -d -v /docker/config/logstash:/config-di
r logstash -f /config-dir/logstash.conf
ac7e137477955fbee6c7af9c5a3f313965a9e0fea79041acfccce6894513055f
[root@ELK ~]#
```

```
docker logs logstash
```

```
[root@ELK ~]# docker logs logstash
Sending Logstash's logs to /var/log/logstash which is now configured via log4j2.properties
00:16:22.132 [main] INFO  logstash.modules.scaffold - Initializing module {:module_name=>"fb_apache", :directory=>"/usr/share/logstash/modules/fb_apache/configuratio
n"}
00:16:22.135 [main] INFO  logstash.modules.scaffold - Initializing module {:module_name=>"netflow", :directory=>"/usr/share/logstash/modules/netflow/configuration"}
00:16:22.137 [main] INFO  logstash.setting.writabledirectory - Creating directory {:setting=>"path.queue", :path=>"/var/lib/logstash/queue"}
00:16:22.138 [main] INFO  logstash.setting.writabledirectory - Creating directory {:setting=>"path.dead_letter_queue", :path=>"/var/lib/logstash/dead_letter_queue"}
00:16:22.152 [LogStash::Runner] INFO  logstash.agent - No persistent UUID file found. Generating new UUID {:uuid=>"53101e8f-e128-4c3c-82b6-cfe0d2ebe320", :path=>"/va
r/lib/logstash/uuid"}
00:16:22.453 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[http://elasticsearch
:9200/]}}
00:16:22.455 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Running health check to see if an Elasticsearch connection is working {:healthcheck_url
=>http://elasticsearch:9200/, :path=>"/"}
00:16:22.576 [[main]-pipeline-manager] WARN  logstash.outputs.elasticsearch - Restored connection to ES instance {:url=>"http://elasticsearch:9200/"}
00:16:22.739 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Using mapping template from {:path=>nil}
00:16:22.741 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Attempting to install template {:manage_template=>{"template"=>"logstash-*", "version"=
>50001, "settings"=>{"index.refresh_interval"=>"5s"}, "mappings"=>{"_default_"=>{"_all"=>{"enabled"=>true, "norms"=>false}, "dynamic_templates"=>[{"message_field"=>{
"path_match"=>"message", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}}, {"string_fields"=>{"match"=>"*", "match_mapping_type"=>"strin
g", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"keyword"=>{"type"=>"keyword", "ignore_above"=>256}}}}}], "properties"=>{"@timestamp"=>{"type"=>"date", "i
nclude_in_all"=>false}, "@version"=>{"type"=>"keyword", "include_in_all"=>false}, "geoip"=>{"dynamic"=>true, "properties"=>{"ip"=>{"type"=>"ip"}, "location"=>{"type"
=>"geo_point"}, "latitude"=>{"type"=>"half_float"}, "longitude"=>{"type"=>"half_float"}}}}}}}
00:16:22.749 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - Installing elasticsearch template to _template/logstash
00:16:22.866 [[main]-pipeline-manager] INFO  logstash.outputs.elasticsearch - New Elasticsearch output {:class=>"LogStash::Outputs::ElasticSearch", :hosts=>["//elast
icsearch:9200"]}
00:16:22.868 [[main]-pipeline-manager] INFO  logstash.pipeline - Starting pipeline {"id"=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipeline.batch.
delay"=>5, "pipeline.max_inflight"=>500}
00:16:23.134 [[main]-pipeline-manager] INFO  logstash.inputs.beats - Beats inputs: Starting input listener {:address=>"0.0.0.0:5044"}
00:16:23.158 [[main]-pipeline-manager] INFO  logstash.pipeline - Pipeline main started
00:16:23.175 [[main]<beats] INFO  org.logstash.beats.Server - Starting server on port: 5044
00:16:23.229 [Api Webserver] INFO  logstash.agent - Successfully started Logstash API endpoint {:port=>9600}
[root@ELK ~]#
```

5. 部署nginx应用

```
docker run -e TZ="Asia/Shanghai" -d -p 80:80 -v "$PWD/logs":/var/log/nginx
--name nginx nginx
```




```
[root@ELK ~]# ls
esdata  logs
[root@ELK ~]# cd logs/
[root@ELK logs]# ls
access.log  error.log
[root@ELK logs]# cat error.log
2021/06/28 08:18:38 [notice] 1#1: using the "epoll" event method
2021/06/28 08:18:38 [notice] 1#1: nginx/1.21.0
2021/06/28 08:18:38 [notice] 1#1: built by gcc 8.3.0 (Debian 8.3.0-6)
2021/06/28 08:18:38 [notice] 1#1: OS: Linux 4.18.0-193.28.1.el8_2.x86_64
2021/06/28 08:18:38 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2021/06/28 08:18:38 [notice] 1#1: start worker processes
2021/06/28 08:18:38 [notice] 1#1: start worker process 31
2021/06/28 08:18:38 [notice] 1#1: start worker process 32
2021/06/28 08:18:38 [notice] 1#1: start worker process 33
2021/06/28 08:18:38 [notice] 1#1: start worker process 34
[root@ELK logs]# cat access.log
[root@ELK logs]# cat access.log
162.105.239.26 - - [28/Jun/2021:08:19:12 +0000] "GET / HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.77 Safari/537.36" "-"
162.105.239.26 - - [28/Jun/2021:08:19:12 +0000] "GET /favicon.ico HTTP/1.1" 404 555 "http://39.105.109.189/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36" "-"
[root@ELK logs]#
```

6. 部署filebeat

```
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.2-x86_64.rpm
```

```
rpm -ivh filebeat-7.4.2-x86_64.rpm
```

```
vim /etc/filebeat/filebeat.yml
```

a. 主要修改下图中红框内标记的配置信息

```bash
grep -Ev '#|^' /etc/filebeat/filebeat.yml
```

```
[root@ELK ~]# grep -Ev '#|^$' /etc/filebeat/filebeat.yml
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /root/logs/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.template.settings:
  index.number_of_shards: 1
setup.kibana:
output.logstash:
  hosts: ["localhost:5044"]
processors:
  - add_host_metadata: ~
  - add_cloud_metadata: ~
[root@ELK ~]#
```

b. 启动filebeat服务

```
systemctl restart filebeat
```

```
systemctl enable filebeat
```

7. 部署kibana

```bash
docker run --name kibana --link elasticsearch:elasticsearch -p 5601:5601 -d kibana
```

```
[root@ELK ~]# docker run --name kibana --link elasticsearch:elasticsearch -p 5601:5601 -d kibana
217e6f38ea4bdf2a37f41240f736e1f81826eeb83fdb20dff49f2a08e8bb6b5c
[root@ELK ~]#
```

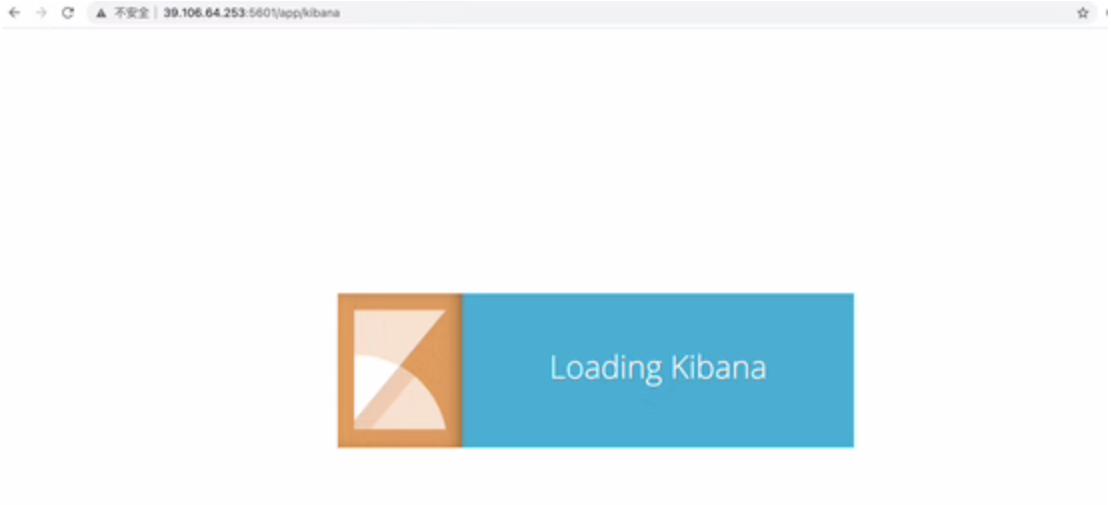
```
[root@ELK ~]# docker logs kibana
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","plugin:kibana@5.6.12","info"],"pid":10,"state":"green","message":"Status changed from uninitializ
ed to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","plugin:elasticsearch@5.6.12","info"],"pid":10,"state":"yellow","message":"Status changed from uni
nitialized to yellow - Waiting for Elasticsearch","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","plugin:console@5.6.12","info"],"pid":10,"state":"green","message":"Status changed from uninitiali
zed to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","plugin:metrics@5.6.12","info"],"pid":10,"state":"green","message":"Status changed from uninitiali
zed to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","plugin:timelion@5.6.12","info"],"pid":10,"state":"green","message":"Status changed from uninitial
ized to green - Ready","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["listening","info"],"pid":10,"message":"Server running at http://0.0.0.0:5601"}
{"type":"log","@timestamp":"2021-06-28T12:52:21Z","tags":["status","ui settings","info"],"pid":10,"state":"yellow","message":"Status changed from uninitialized to ye
llow - Elasticsearch plugin is yellow","prevState":"uninitialized","prevMsg":"uninitialized"}
{"type":"log","@timestamp":"2021-06-28T12:52:26Z","tags":["status","plugin:elasticsearch@5.6.12","info"],"pid":10,"state":"yellow","message":"Status changed from yel
low to yellow - No existing Kibana index found","prevState":"yellow","prevMsg":"Waiting for Elasticsearch"}
[root@ELK ~]#
```

```bash
docker ps -a
```

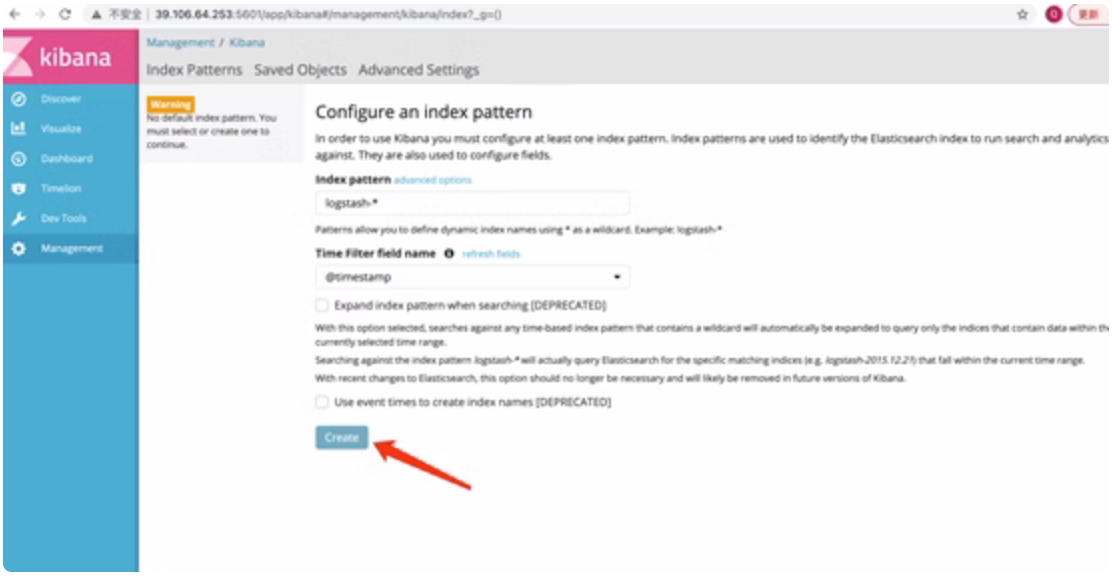
```
[root@ELK ~]# docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS          PORTS                                                   NAMES
217e6f38ea4b   kibana         "/docker-entrypoint.…"   2 minutes ago    Up 2 minutes    0.0.0.0:5601->5601/tcp, :::5601->5601/tcp               kibana
c13cabb67534   nginx          "/docker-entrypoint.…"   17 minutes ago   Up 17 minutes   0.0.0.0:80->80/tcp, :::80->80/tcp                       nginx
ac7e13747795   logstash       "/docker-entrypoint.…"   20 minutes ago   Up 20 minutes   0.0.0.0:5044->5044/tcp, :::5044->5044/tcp               logstash
bf100ae0fd6d   elasticsearch  "/docker-entrypoint.…"   20 minutes ago   Up 20 minutes   0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp     elasticsearch
[root@ELK ~]#
```

访问kibana http://39.106.64.253:5601/

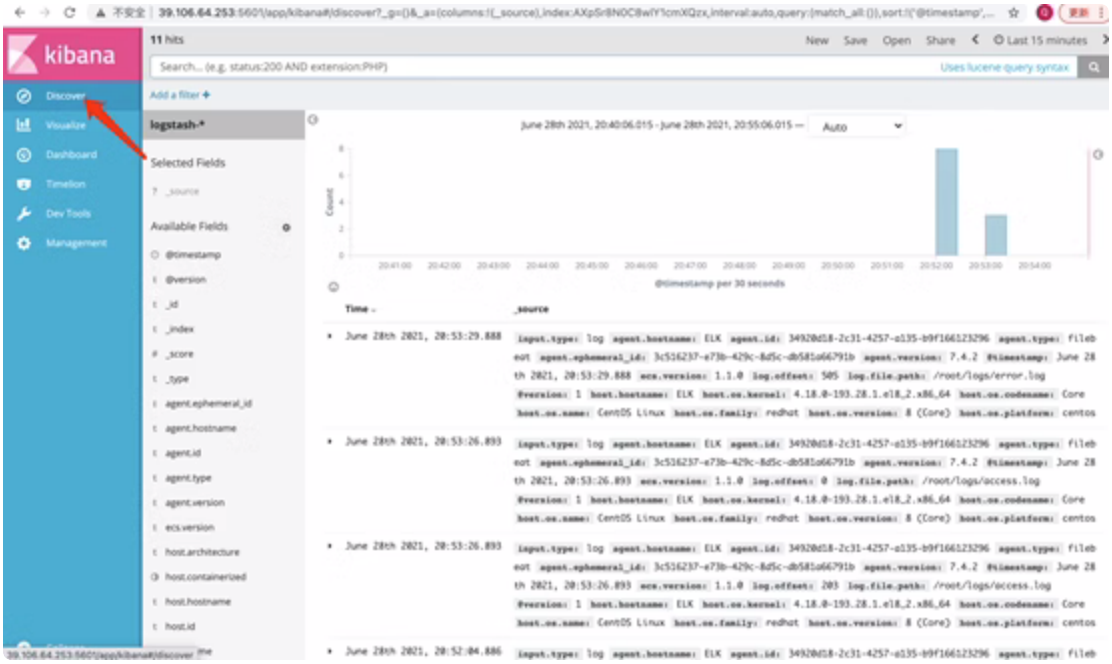
注意：这里的IP地址需要换成实验服务器公网IP地址。



创建Index pattern



查看采集到的日志信息


kibana
11 hits
New Save Open Share
Last 15 minutes
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
logstash-*
Selected Fields
_source
Available Fields
@timestamp
@version
_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version
ecs.version
host.architecture
host.containerized
host.hostname
host.id
June 28th 2021, 20:40:06.015 - June 28th 2021, 20:55:06.015 —
Auto
Count
@timestamp per 30 seconds
Time
_source