ZHUYUN

# ELK on CentOS 7.2
# User’s Guide

| Revision History | | | |
|---|---|---|---|
| Date | Version | Description | Prepared by |
| 2017/09/01 | V1.1 | User’s Guide | Zhuyun/Technical Support |

Zhuyun Information Technology Co.,Ltd.
www.cloudcare.cn

# Contents

# Preface

## I. Copyright:

1、 All contents provided in this document, including images, texts, pictures, software, and programs are properties of Shanghai Zhuyun Information Technology Co., Ltd. ("the Company"). All rights reserved.

2、Visitors may use the content or services provided in this document for personal study, research, and other non-commercial or non-profit uses, but they shall comply with the Copyright Law and other related laws and shall not infringe the legal rights of the Company. No organization or individual may apply any content or service of this document to any other occasions without prior written consent of the Company. The Company shall hold any organization or individual accountable by law for any unauthorized use of this document.

3. If you have other suggestions on image, send them to support@jiagouyun.com.

## II. About us:

Zhuyun Information Technology Co., Ltd. was founded in 2013, as one of the few services companies entirely engaged in cloud-based business in China. Relying on Alibaba Cloud's public cloud computing technology, Zhuyun is committed to helping the majority of companies choose the cloud and big data products that truly fit their business needs. Meanwhile. Zhuyun provides services including consulting, design, system implementation, application migration, system management, hybrid cloud management, and data center construction and other services; and helps enterprises build IT infrastructure of the cloud computing era.

## III. Contact us:

1. Website

http://www.cloudcare.cn

2. Address

No. 399 Keyuan Road, Pudong District, Shanghai (Headquarters)

Hangzhou Intelligent Industrial Incubator, No. 857 West Wenyi Road, Xihu District, Hangzhou

Yinhe SOHO, Chaoyangmen, Dongcheng District, Beijing

Zhonghua Plaza, No. 33 of Third Zhongshan Road, Yuexiu District, Guangzhou

Zhongguancun Software Park, No.7 Yingcui Road, Jiangning District, Nanjing

Tianfu Software Park, No.216 Century City South Road, High-tech Zone, Chengdu

3. More support and help

Tel: 021-50800099

Technical support: 021-50800099-103

TradeManager: Architecture Cloud

Email: support@jiagouyun.com

# 1. Image environment

## 1.1. Image version

Operating System: Centos 7.2 64 bits

Software details of the image V1.0:

elasticsearch-5.2.1 + Logstash-5.2-1 + kibana-5.2.1

## 1.2. Installation instructions

The image enviroment is installed by official rpm package, which is downloaded from the official website(www.elastic.co).

In the image, scripts about installation and uninstallation are both under directory “/root/elk_update” .

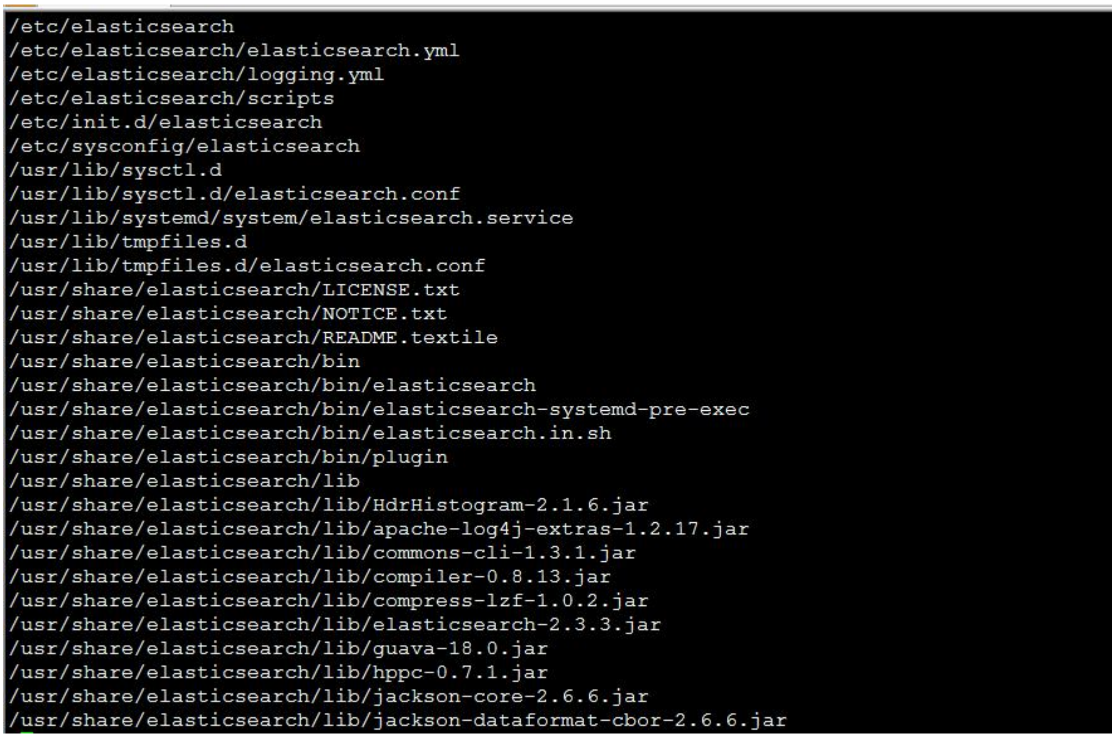
# 2. Software directories and configuration list

The ELK software is installed with official rpm package and installed into default directories:

Elasticsearch configuration file: /etc/elasticsearch/elasticsearch.yml

Elasticsearch log directory: /var/log/elasticsearch

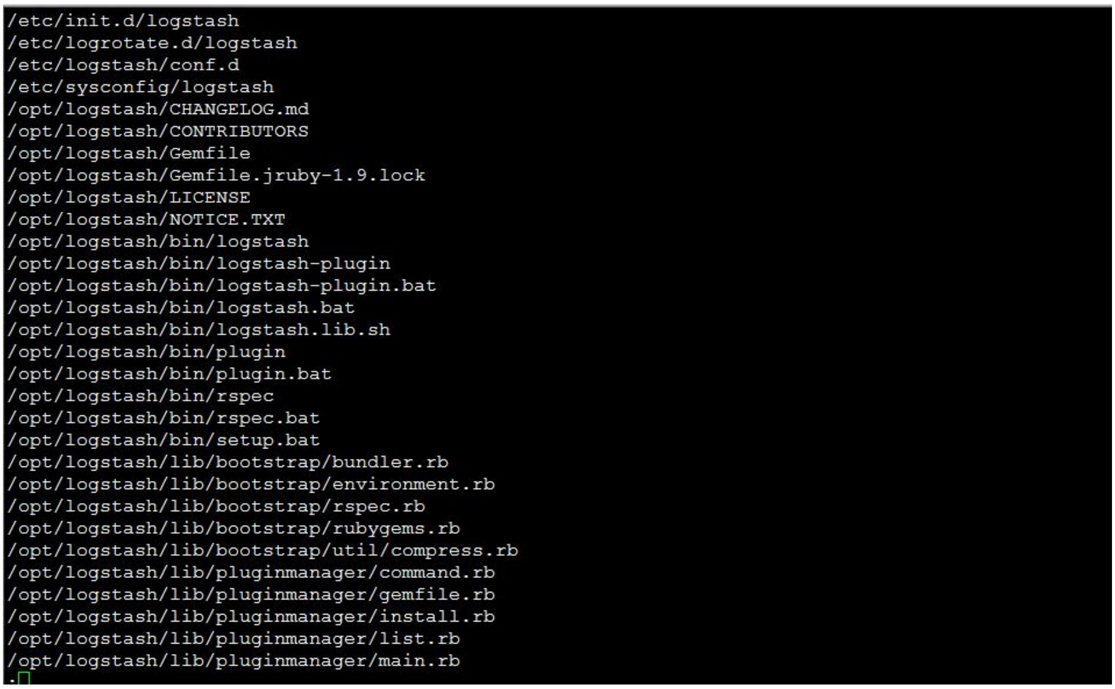
More related directories and documents can be seen below:



```
/etc/elasticsearch
/etc/elasticsearch/elasticsearch.yml
/etc/elasticsearch/logging.yml
/etc/elasticsearch/scripts
/etc/init.d/elasticsearch
/etc/sysconfig/elasticsearch
/usr/lib/sysctl.d
/usr/lib/sysctl.d/elasticsearch.conf
/usr/lib/systemd/system/elasticsearch.service
/usr/lib/tmpfiles.d
/usr/lib/tmpfiles.d/elasticsearch.conf
/usr/share/elasticsearch/LICENSE.txt
/usr/share/elasticsearch/NOTICE.txt
/usr/share/elasticsearch/README.textile
/usr/share/elasticsearch/bin
/usr/share/elasticsearch/bin/elasticsearch
/usr/share/elasticsearch/bin/elasticsearch-systemd-pre-exec
/usr/share/elasticsearch/bin/elasticsearch.in.sh
/usr/share/elasticsearch/bin/plugin
/usr/share/elasticsearch/lib
/usr/share/elasticsearch/lib/HdrHistogram-2.1.6.jar
/usr/share/elasticsearch/lib/apache-log4j-extras-1.2.17.jar
/usr/share/elasticsearch/lib/commons-cli-1.3.1.jar
/usr/share/elasticsearch/lib/compiler-0.8.13.jar
/usr/share/elasticsearch/lib/compress-lzf-1.0.2.jar
/usr/share/elasticsearch/lib/elasticsearch-2.3.3.jar
/usr/share/elasticsearch/lib/guava-18.0.jar
/usr/share/elasticsearch/lib/hppc-0.7.1.jar
/usr/share/elasticsearch/lib/jackson-core-2.6.6.jar
/usr/share/elasticsearch/lib/jackson-dataformat-cbor-2.6.6.jar
```

Logstash configuration file: /etc/logstash/conf.d/ (Note: logstash require users to manually edit the configuration file based on their actual environment).

Since many files and directories generated, here will not list anymore, refer to below to get more:



```
/etc/init.d/logstash
/etc/logrotate.d/logstash
/etc/logstash/conf.d
/etc/sysconfig/logstash
/opt/logstash/CHANGELOG.md
/opt/logstash/CONTRIBUTORS
/opt/logstash/Gemfile
/opt/logstash/Gemfile.jruby-1.9.lock
/opt/logstash/LICENSE
/opt/logstash/NOTICE.TXT
/opt/logstash/bin/logstash
/opt/logstash/bin/logstash-plugin
/opt/logstash/bin/logstash-plugin.bat
/opt/logstash/bin/logstash.bat
/opt/logstash/bin/logstash.lib.sh
/opt/logstash/bin/plugin
/opt/logstash/bin/plugin.bat
/opt/logstash/bin/rspec
/opt/logstash/bin/rspec.bat
/opt/logstash/bin/setup.bat
/opt/logstash/lib/bootstrap/bundler.rb
/opt/logstash/lib/bootstrap/environment.rb
/opt/logstash/lib/bootstrap/rspec.rb
/opt/logstash/lib/bootstrap/rubygems.rb
/opt/logstash/lib/bootstrap/util/compress.rb
/opt/logstash/lib/pluginmanager/command.rb
/opt/logstash/lib/pluginmanager/gemfile.rb
/opt/logstash/lib/pluginmanager/install.rb
/opt/logstash/lib/pluginmanager/list.rb
/opt/logstash/lib/pluginmanager/main.rb
```

# 3. Command summary

systemctl start (start stop restart) logstash

systemctl start (start stop restart) kibana

systemctl start (start stop restart) elasticsearch

# 4. Uninstalling ELK

Refer to below commands to uninstall ELK software:

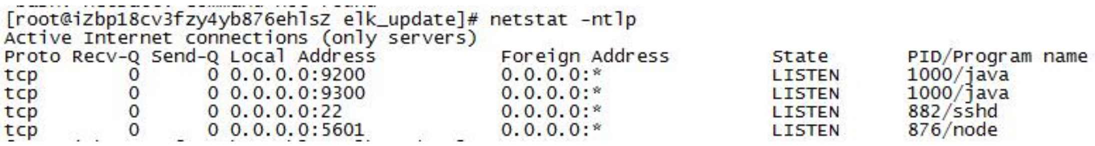
[redacted]

Or use uninstallation script under “/root/elk_update/” directory.

Note: This operation will clean up the environment of the image. Before uninstalling, please back up necessary data.

# 5. Default settings of the image

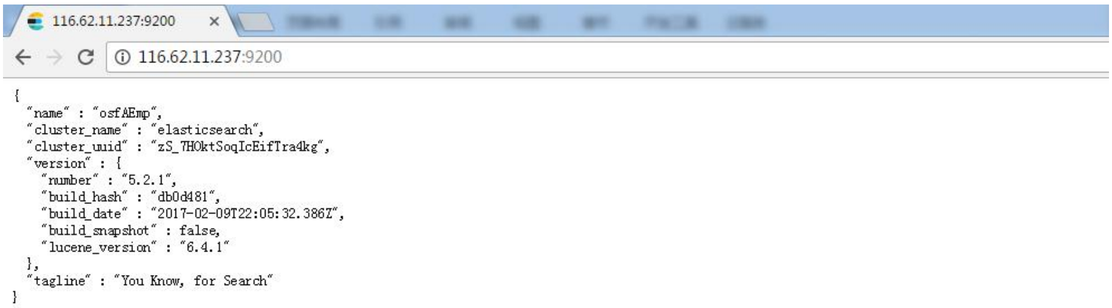
In the image, elasticsearch listens on port 9200, logstash listens on port 9300, kibana listens on port 5601. The related ports will be listened on automatically once the image installation done, indicating that the ELK infrastructure is deployed (users can edit the configuration file to change the listening ports according to the situation).



```
[root@izbp18cv3fzy4yb876ehlsz elk_update]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9200            0.0.0.0:*               LISTEN      1000/java
tcp        0      0 0.0.0.0:9300            0.0.0.0:*               LISTEN      1000/java
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      882/sshd
tcp        0      0 0.0.0.0:5601            0.0.0.0:*               LISTEN      876/node
```

After deploying image done, test it through visiting IP+port in browser. The following figure is a simple example, and more operations should be based on the actual situation.

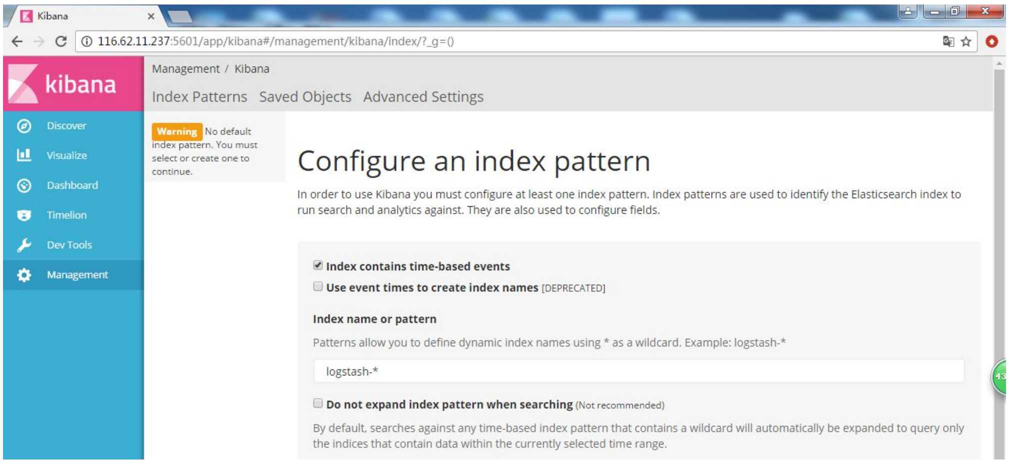
Elasticsearch



```
{
  "name" : "osfAEmp",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "zS_7HOktSoqIcEifTra4kg",
  "version" : {
    "number" : "5.2.1",
    "build_hash" : "db0d481",
    "build_date" : "2017-02-09T22:05:32.386Z",
    "build_snapshot" : false,
    "lucene_version" : "6.4.1"
  },
  "tagline" : "You Know, for Search"
}
```

Kibana

Note that users need to create an index schema or select an existing index schema on this page. For more information, refer to the web browser.



Warning No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☑ Index contains time-based events

□ Use event times to create index names [DEPRECATED]

Index name or pattern

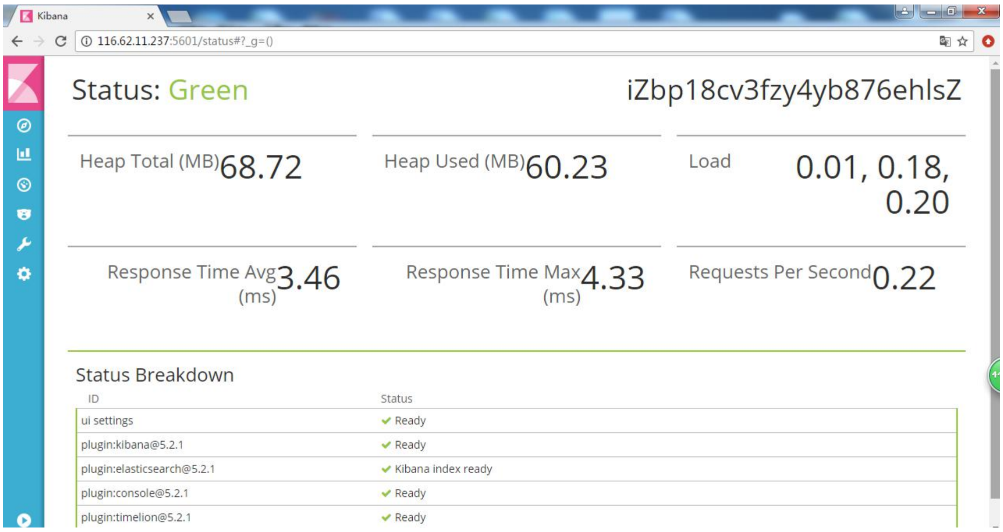
Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

logstash-*

□ Do not expand index pattern when searching (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

You can see the status of kibana service from below figure.



Status: Green

iZbp18cv3fzy4yb876ehlsZ

Heap Total (MB) 68.72

Heap Used (MB) 60.23

Load 0.01, 0.18, 0.20

Response Time Avg (ms) 3.46

Response Time Max (ms) 4.33

Requests Per Second 0.22

Status Breakdown

| ID | Status |
|---|---|
| ui settings | ✓ Ready |
| plugin:kibana@5.2.1 | ✓ Ready |
| plugin:elasticsearch@5.2.1 | ✓ Kibana index ready |
| plugin:console@5.2.1 | ✓ Ready |
| plugin:timelion@5.2.1 | ✓ Ready |