

logstash

filebeat 和 logstash

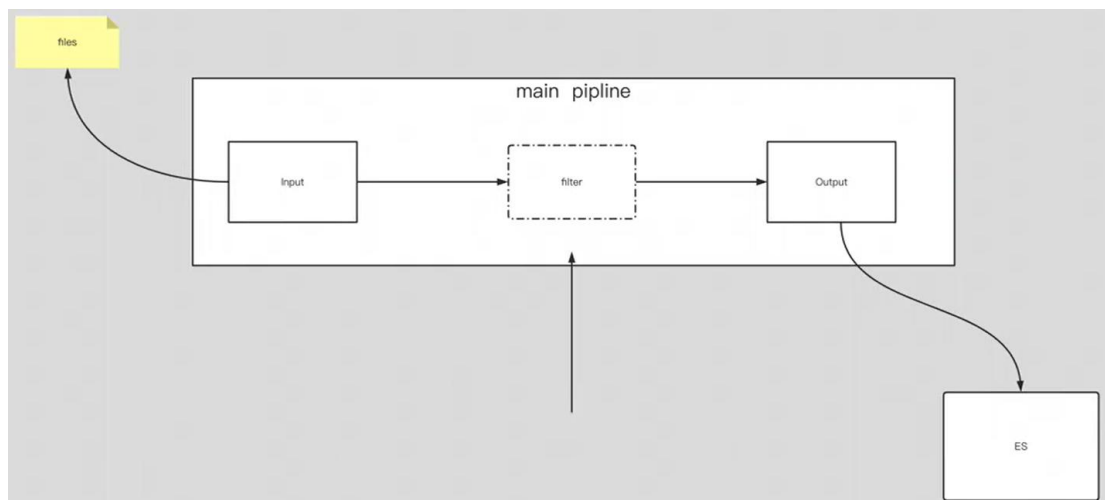
因为 logstash 是 jvm 跑的，资源消耗比较大，所以后来作者又用 golang 写了一个功能较少但是资源消耗也小的轻量级的 logstash-forwarder。不过作者只是一个人，加入 <http://elastic.co> 公司以后，因为 es 公司本身还收购了另一个开源项目 packetbeat，而这个项目专门就是用 golang 的，有整个团队，所以 es 公司干脆把 logstash-forwarder 的开发工作也合并到同一个 golang 团队来搞，于是新的项目就叫 filebeat 了。

logstash 和 filebeat 都具有日志收集功能，filebeat 更轻量，占用资源更少，但 logstash 具有 filter 功能，能过滤分析日志。一般结构都是 filebeat 采集日志，然后发送到消息队列，redis，kafaka。然后 logstash 去获取，利用 filter 功能过滤分析，然后存储到 elasticsearch 中

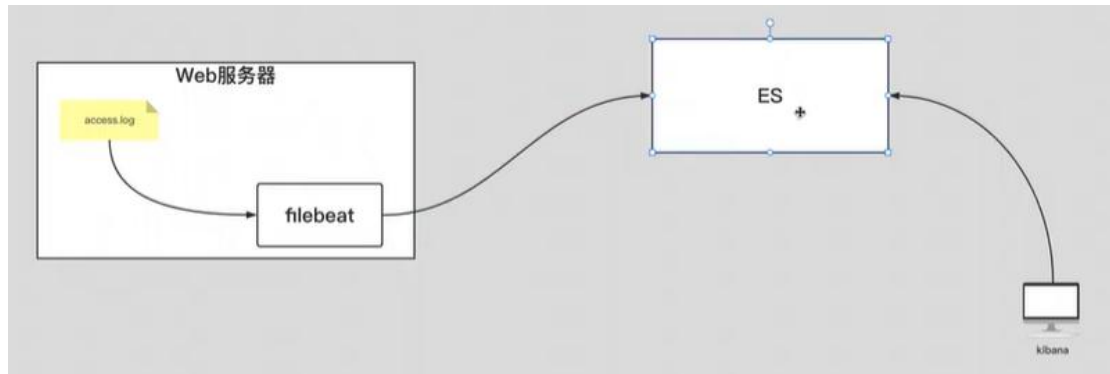
logstash 的安装包要比 filebeat 大的多

```
-rw-r--r-- 1 root root 347M Apr 20 21:18 logstash-7.17.3-linux-x86_64.tar.gz
-rw-r--r-- 1 root root 35M Apr 20 21:00 filebeat-7.17.3-linux-x86_64.tar.gz
```

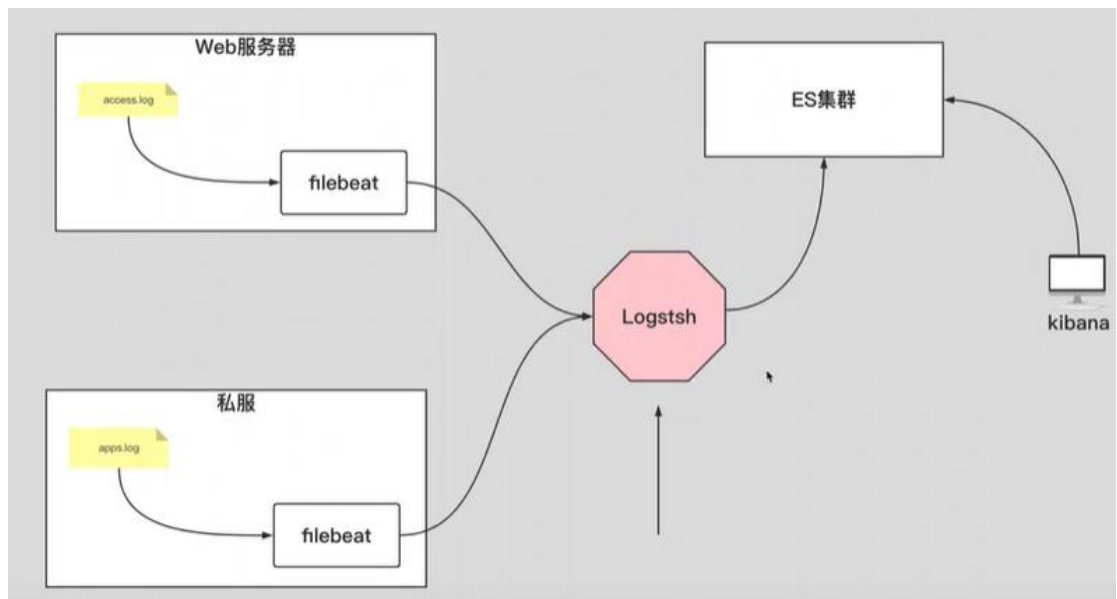
logstash 和 filebeat 都有输入和输出，但是 logstash 比 filebeat 多了个 filter 的功能,该功能就是 logstash 的强大之处



简单的数据处理



需要对数据进度分析处理



logstash 部署

文档

<https://www.elastic.co/guide/en/logstash/current/plugins-outputs-elasticsearch.html>

elastic

PlatformSolutionsCustomersResourcesPricingDocs

Transforming Data

Deploying and Scaling Logstash

Managing GeolIP Databases

Performance Tuning

Monitoring Logstash with Elastic Agent

Monitoring Logstash (legacy)

Monitoring Logstash with APIs

Working with plugins

Integration plugins

Input plugins

Output plugins

Filter plugins

Codec plugins

Tips and best practices

Troubleshooting

Contributing to Logstash

Contributing a Java Plugin

Breaking changes

Elastic Docs > Logstash Reference [8.13] > Output plugins

Elasticsearch output plugin

- Plugin version: v11.22.5
- Released on: 2024-04-02
- Changelog

For other versions, see the [Versioned plugin docs](#).

Getting Help

For questions about the plugin, open a topic in the [Discuss](#) forums. For bugs or feature requests, open an issue in [Github](#). For the list of Elastic supported plugins, please consult the [Elastic Support Matrix](#).

Description

Elasticsearch provides near real-time search and analytics for all types of data. The Elasticsearch output plugin can store both time series datasets (such as logs, events, and metrics) and non-time series data in Elasticsearch.

You can [learn more about Elasticsearch](#) on the website landing page or in the [Elasticsearch documentation](#).

NOTE

Compatibility Note

When connected to Elasticsearch 7.x, modern versions of this plugin don't use the document-type when inserting documents, unless the user explicitly sets `document_type`.

If you are using an earlier version of Logstash and wish to connect to Elasticsearch 7.x, first upgrade Logstash to version 6.8 to ensure it picks up changes to the Elasticsearch index template.

If you are using a custom [template](#), ensure your template uses the `_doc` document-type before connecting to Elasticsearch 7.x.

On this page

[Getting Started](#)

[Description](#)

[Logstash server](#)

[Hosted on Elastic](#)

[Compare](#)

[Comments](#)

[Data stream](#)

[Data export](#)

[Writing best practices](#)

[Retry Policy](#)

[DLO Policy](#)

[More](#)

[Videos](#)

[Get started](#)

[Elasticsearch](#)

[Videos](#)

[Intro](#)

[Videos](#)

[ELK](#)

[Was](#)

安装

```
yum -y localinstall logstash-7.17.3-x86_64.rpm

ln -sv /usr/share/logstash/bin/logstash /usr/local/bin/

下载地址:
https://www.elastic.co/downloads/past-releases#logstash
```

修改 logstash 的配置文件

```
(1)编写配置文件
cat > conf.d/01-stdin-to-stdout.conf <<'EOF'
input {
  stdin {}
}

output {
  stdout {}
}
EOF

(2)检查配置文件语法
logstash -tf conf.d/01-stdin-to-stdout.conf

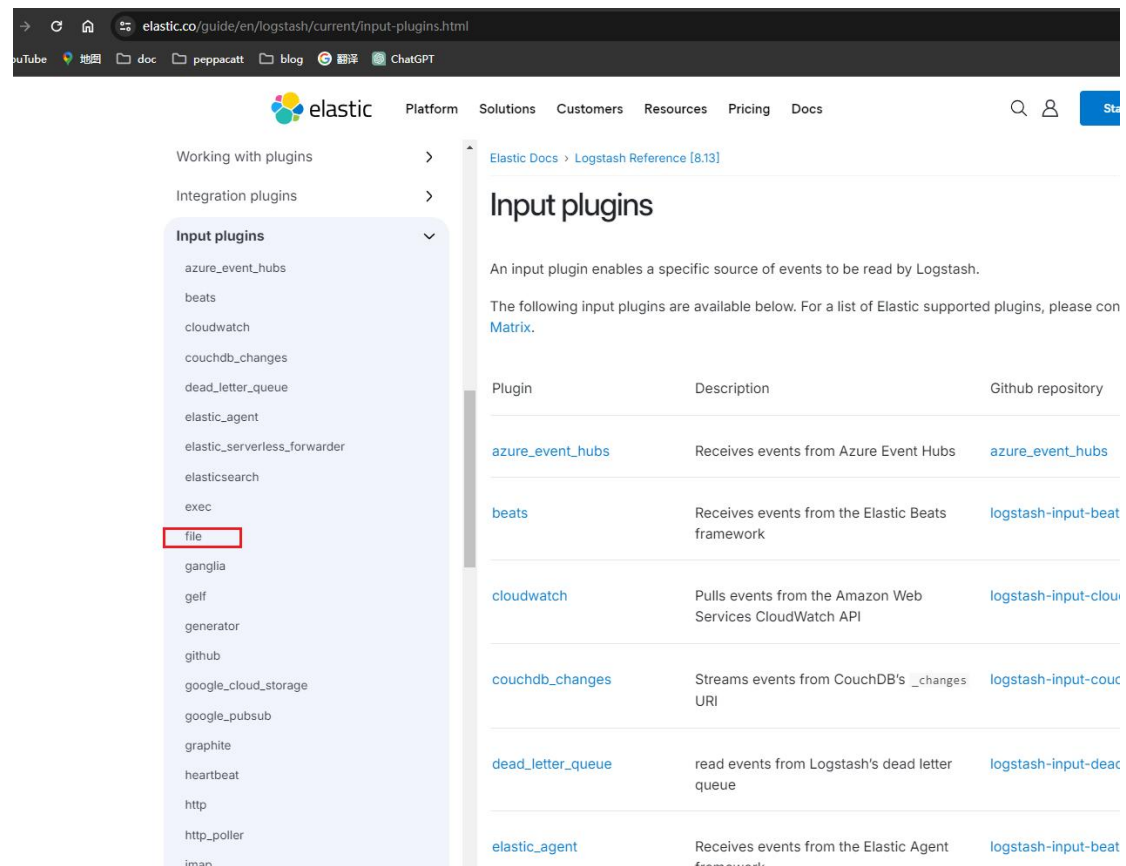
(3)启动logstash实例
logstash -f conf.d/01-stdin-to-stdout.conf
```

其中 -t 是 test 的意思

-r 热加载, logstash 的启动比较耗时,加上-r 参数后,修改配置文件后不用重启

input 插件

input->file



Working with plugins

Integration plugins

Input plugins

- azure_event_hubs
- beats
- cloudwatch
- couchdb_changes
- dead_letter_queue
- elastic_agent
- elastic_serverless_forwarder
- elasticsearch
- exec
- file
- ganglia
- gelf
- generator
- github
- google_cloud_storage
- google_pubsub
- graphite
- heartbeat
- http
- http_poller
- imn

Input plugins

An input plugin enables a specific source of events to be read by Logstash.

The following input plugins are available below. For a list of Elastic supported plugins, please con[Matrix](#).

Plugin	Description	Github repository
azure_event_hubs	Receives events from Azure Event Hubs	azure_event_hubs
beats	Receives events from the Elastic Beats framework	logstash-input-beat
cloudwatch	Pulls events from the Amazon Web Services CloudWatch API	logstash-input-clou
couchdb_changes	Streams events from CouchDB's <code>_changes</code> URI	logstash-input-couc
dead_letter_queue	read events from Logstash's dead letter queue	logstash-input-deac
elastic_agent	Receives events from the Elastic Agent framework	logstash-input-beat

input 中的插件 file

```
total 1319984
drwxr-xr-x 2 root root 4096 May 12 12:22 config-logstash
drwxr-xr-x 2 root root 4096 May 10 20:27 day01-基础设施及部署文件
-rw-r--r-- 1 root root 311777007 Apr 20 21:08 elasticsearch-7.17.3-linux-x86_64.tar.gz
-rw-r--r-- 1 root root 311873551 Apr 20 21:09 elasticsearch-7.17.3-x86_64.rpm
-rw-r--r-- 1 root root 363469045 Apr 20 21:18 logstash-7.17.3-linux-x86_64.tar.gz
-rw-r--r-- 1 root root 364517723 Apr 20 21:20 logstash-7.17.3-x86_64.rpm
[root@elk101.oidboyedu.com ~]#
[root@elk101.oidboyedu.com ~]#
[root@elk101.oidboyedu.com ~]# cp config-logstash/01-stdin-to-stdout.conf config-logstash/02-file-to-stdout.conf
[root@elk101.oidboyedu.com ~]#
[root@elk101.oidboyedu.com ~]# vim config-logstash/02-file-to-stdout.conf
[root@elk101.oidboyedu.com ~]#
[root@elk101.oidboyedu.com ~]#
[root@elk101.oidboyedu.com ~]# logstash -f config-logstash/02-file-to-stdout.conf
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continue
Could not find logstash configuration at path /usr/share/logstash/config/logstash42.properties. Using default config which logs errors to the console
[INFO ] 2022-05-12 14:36:22.050 [main] runner - Starting Logstash ("logstash.version"=>"7.17.3", "jruby.version"=>"jruby 9.2.20.1 (2.5.8) 2021-11-30 2a296
t Server VM 11.0.14.1-i on 11.0.14.1-i *indy *jit [linux-x86_64]")
[INFO ] 2022-05-12 14:36:22.136 [main] runner - JVM bootstrap flags: [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:
cupancyOnly, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.invokedynamic=true, -Djruby.jit.threshold=0, -Djruby.regex.interruptible=tr
OutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true]
[WARN ] 2022-05-12 14:36:22.591 [Logstash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2022-05-12 14:36:23.642 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
[INFO ] 2022-05-12 14:36:24.397 [Converge PipelineAction::Create<main>] Reflections - Reflections took 56 ms to scan 1 urls, producing 119 keys and 419 va
[WARN ] 2022-05-12 14:36:24.988 [Converge PipelineAction::Create<main>] plain - Relying on default value of 'pipeline.ecs_compatibility', which may change
release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
[WARN ] 2022-05-12 14:36:25.022 [Converge PipelineAction::Create<main>] file - Relying on default value of 'pipeline.ecs_compatibility', which may change
release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
[INFO ] 2022-05-12 14:36:25.244 [main]-pipeline-manager] jvapiipeline - Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>2, "pipeline.batch.s
e.batch.delay"=>50, "pipeline.max_inflight"=>250, "pipeline.sources"=>["/root/.config-logstash/02-file-to-stdout.conf"]}, :thread=>"#<Thread:0x78c44e51 run>
[INFO ] 2022-05-12 14:36:25.870 [main]-pipeline-manager] jvapiipeline - Pipeline Java execution initialization time {"seconds"=>0.62}
[INFO ] 2022-05-12 14:36:25.961 [main]-pipeline-manager] file - No sincedb_path set, generating one based on the "path" setting {:sincedb_path=>"/usr/sha
ugins/inputs/file/.sincedb_3cd99a80ca58225ec14dc0ac340abb80", :path=>"/tmp/test/*.txt"}
[INFO ] 2022-05-12 14:36:25.980 [main]-pipeline-manager] jvapiipeline - Pipeline started {"pipeline.id"=>"main"}
```

```

(1)编写logstash的配置文件
cat > conf.d/02-file-to-stdout <<'EOF'
input {
  file {
    # 指定收集的路径
    path => ["/tmp/test/*.txt"]
    # 指定文件的读取位置, 仅在第一次生效.
    start_position => "beginning"
  }
}

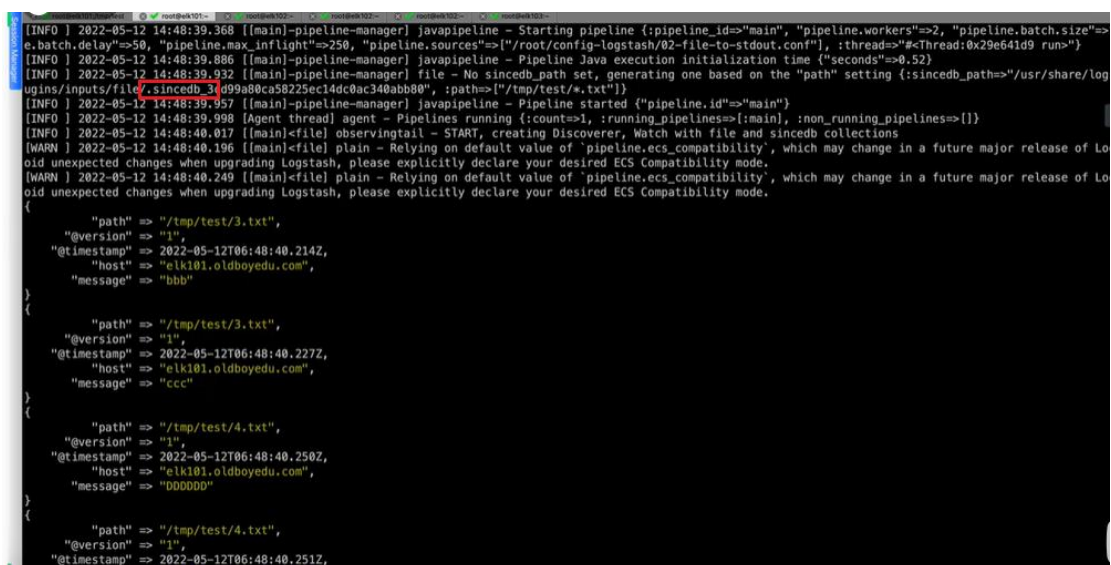
output {
  stdout {}

  # elasticsearch {
  # }
}
EOF

(2)启动logstash实例
logstash -rf conf.d/02-file-to-stdout

```

已读取过的文件会在 `sincedb` 中产生记录, `start_position` 为 `beginning` 时, 读取的是在 `sincedb` 中没有记录的文件



```

[INFO ] 2022-05-12 14:48:39.368 [main]-pipeline-manager jvavapipeline - Starting pipeline {:pipeline_id=>"main", "pipeline.workers">2, "pipeline.batch.size">50, "pipeline.batch.delay">50, "pipeline.max_inflight">250, "pipeline.sources">["/root/.config-logstash/02-file-to-stdout.conf"]}, :thread=>#<Thread:0x29e641d9 run>}
[INFO ] 2022-05-12 14:48:39.886 [main]-pipeline-manager jvavapipeline - Pipeline Java execution initialization time {"seconds">0.52}
[INFO ] 2022-05-12 14:48:39.932 [main]-pipeline-manager file - No sincedb_path set, generating one based on the "path" setting {:sincedb_path=>"/usr/share/logstash/inputs/file/.sincedb_3d99a80ca58225ec14dc0ac340abb80", :path=>["/tmp/test/*.txt"]}
[INFO ] 2022-05-12 14:48:39.957 [main]-pipeline-manager jvavapipeline - Pipeline started {"pipeline.id">"main"}
[INFO ] 2022-05-12 14:48:39.998 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>{:main}, :non_running_pipelines=>[]}
[INFO ] 2022-05-12 14:48:40.017 [main]<file> observingtail - START, creating Discoverer, Watch with file and sincedb collections
[WARN ] 2022-05-12 14:48:40.196 [main]<file> plain - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
[WARN ] 2022-05-12 14:48:40.249 [main]<file> plain - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
{
  "path" => "/tmp/test/3.txt",
  "@version" => "1",
  "@timestamp" => 2022-05-12T06:48:40.214Z,
  "host" => "elk101.oldboyedu.com",
  "message" => "bbb"
}
{
  "path" => "/tmp/test/3.txt",
  "@version" => "1",
  "@timestamp" => 2022-05-12T06:48:40.227Z,
  "host" => "elk101.oldboyedu.com",
  "message" => "ccc"
}
{
  "path" => "/tmp/test/4.txt",
  "@version" => "1",
  "@timestamp" => 2022-05-12T06:48:40.250Z,
  "host" => "elk101.oldboyedu.com",
  "message" => "DDDDDD"
}
{
  "path" => "/tmp/test/4.txt",
  "@version" => "1",
  "@timestamp" => 2022-05-12T06:48:40.251Z,
  "host" => "elk101.oldboyedu.com",
  "message" => "DDDDDD"
}

```

input->tcp

tcp 使用场景

对于不支持安装客户端的交换机和路由器, 可以先通过 `tcp` 将日志发到指定端口, 由 `logstash` 聚合

结果

```
[root@elk101.oldboyedu.com ~]# cp config-logstash/02-file-to-stdout.conf config-logstash/03-tcp-to-stdout.conf
[root@elk101.oldboyedu.com ~]#
[root@elk101.oldboyedu.com ~]# vim config-logstash/03-tcp-to-stdout.conf
[root@elk101.oldboyedu.com ~]#
[root@elk101.oldboyedu.com ~]# logstash -f config-logstash/03-tcp-to-stdout.conf
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
WARNING: Could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console
[INFO ] 2022-05-12 15:07:23.019 [main] runner - Starting Logstash ("logstash.version"=>"7.17.3", "ruby.version"=>"ruby 9.2.20.1 (2.5.8) 2021-11-30 2a29
t Server VM 11.0.14.1+1 on 11.0.14.1+1 +indy +jit [linux-x86_64]")
[INFO ] 2022-05-12 15:07:23.061 [main] runner - JVM bootstrap flags: [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX
cupancyOnly, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.invokedynamic=true, -Djruby.jit.threshold=0, -Djruby.regexp.interruptible=
OutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true]
[WARN ] 2022-05-12 15:07:23.779 [LogStash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2022-05-12 15:07:25.288 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
[INFO ] 2022-05-12 15:07:25.614 [Converge PipelineAction::Create<main>] Reflections - Reflections took 75 ms to scan 1 urls, producing 119 keys and 419 v
[WARN ] 2022-05-12 15:07:26.162 [Converge PipelineAction::Create<main>] line - Relying on default value of 'pipeline.ecs_compatibility', which may change
elease of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
[WARN ] 2022-05-12 15:07:26.184 [Converge PipelineAction::Create<main>] tcp - Relying on default value of 'pipeline.ecs_compatibility', which may change
elease of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
[INFO ] 2022-05-12 15:07:26.396 [main-pipeline-manager] jvapipline - Starting pipeline {pipeline_id=>"main", "pipeline.workers"=>2, "pipeline.batch
e_batch.delay"=>50, "pipeline.max_inflight"=>250, "pipeline.sources"=>["/root/.config-logstash/03-tcp-to-stdout.conf"]}, :threads=>#{Thread:0x38e3bcc4 run
[INFO ] 2022-05-12 15:07:27.194 [main-pipeline-manager] jvapipline - Pipeline Java execution initialization time {"seconds"=>0.0}
[INFO ] 2022-05-12 15:07:27.423 [main-pipeline-manager] jvapipline - Pipeline started {"pipeline_id"=>"main"}
[INFO ] 2022-05-12 15:07:27.454 [agent thread] agent - Pipelines running (:count=>1, :running_pipelines=>{:main}, :non_running_pipelines=>[])
[INFO ] 2022-05-12 15:07:27.498 [main-tcp] tcp - Starting tcp input listener {:address=>"0.0.0.0:8888", :ssl_enabled=>false}
[WARN ] 2022-05-12 15:07:52.073 [nioEventLoopGroup-2-1] line - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future maj
sh. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.
{
  "port" => 44482,
  "@version" => "1",
  "host" => "elk103.oldboyedu.com",
  "message" => "aaaaaaaaaaaaaaaaaaaaaa",
  "@timestamp" => 2022-05-12T07:07:58.184Z
}
```

input->http

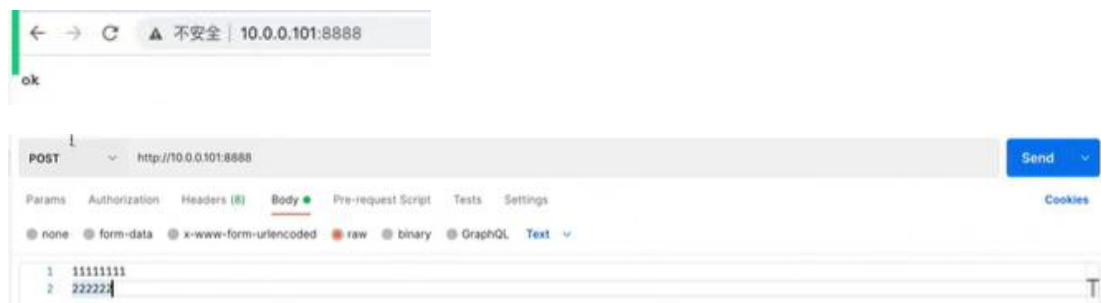
http 和 tcp 在 7 层协议中对应的层级不同

```
[root@elk101.oldboyedu.com ~]# cat config-logstash/04-http-to-stdout.conf
input {
  http {
    port => 8888
  }

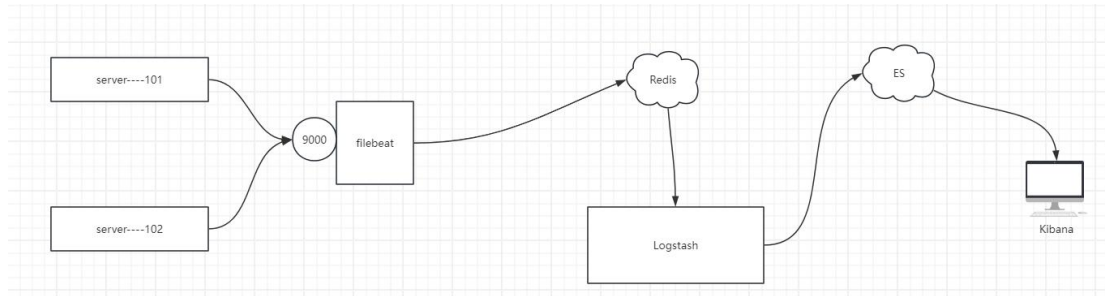
  http {
    port => 9999
  }
}

output {
  stdout {}
}
[root@elk101.oldboyedu.com ~]#
[root@elk101.oldboyedu.com ~]#
[root@elk101.oldboyedu.com ~]# logstash -f config-logstash/04-http-to-stdout.conf
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
```

发送数据测试(可使用 postman)



input->redis



```
input {
  redis {
    # 指定的是REDIS的键(key)的类型
    data_type => "list"
    # 指定数据库的编号,默认值是0号数据库
    db => 5
    # 指定数据库的ip地址,默认值是localhost
    host => "10.0.0.101"
    # 指定数据库的端口号,默认值为6379
    port => 6379
    # 指定redis的认证密码
    password => "oldboyedu"
    # 指定从redis的哪个key取数据
    key => "oldboyedu-linux80-filebeat"
  }
}

output {
  stdout {}
}
```

input->beats

filebeat 输出到 logstash

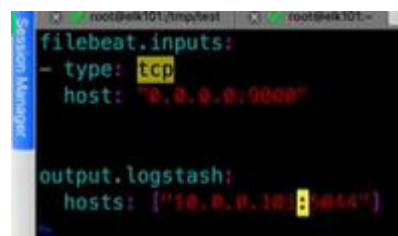
```
filebeat配置:
filebeat.inputs:
- type: tcp
  host: "0.0.0.0:9000"

output.logstash:
  hosts: ["10.0.0.101:5044"]

logstash配置:
input {
  beats {
    port => 5044
  }
}

output {
  stdout {}
}
```


filebeat 配置修改



```
filebeat.inputs:
- type: tcp
  host: "0.0.0.0:9000"

output.logstash:
  hosts: ["10.0.0.101:5044"]
```

logstash 配置修改

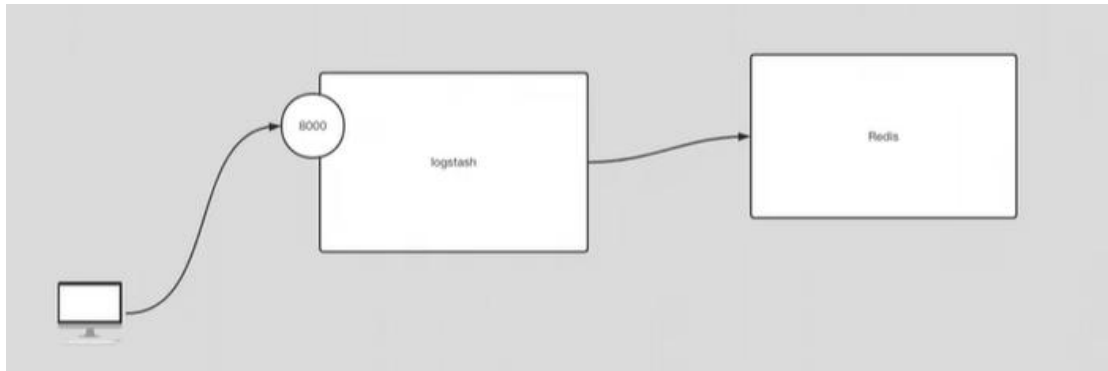


```
input {
  beats {
    port => 5044
  }
}

output {
  stdout {}
}
```

output 插件

output->redis



```
input {
  tcp {
    port => 9999
  }
}

output {
  stdout {}

  redis {
    # 指定redis的主机地址
    host => "10.0.0.101"
    # 指定redis的端口号
    port => "6379"
    # 指定redis数据库编号
    db => 10
    # 指定redis的密码
    password => "oldboyedu"
    # 指定写入数据的key类型
    data_type => "list"
    # 指定的写入的key名称
    key => "oldboyedu-linux80-logstash"
  }
}
```

```
[root@elk101.oldboyedu.com ~]# logstash -f config-logstash/07-tcp-to-redis.conf
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
```

output->file

```
input {  
  tcp {  
    port => 9999  
  }  
}  
  
output {  
  stdout {}  
  
  file {  
    # 指定磁盘的落地位置  
    path => /tmp/oldboyedu-linux80-logstash.log  
  }  
}
```