Download and install Filebeat

Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, **Filebeat** monitors the log files or locations that you specify, collects log events, and forwards them to either to Elasticsearch or Logstash for indexing.

1 .Downloading and installing filebeat

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.1.1-x86_64.rpm sudo rpm -vi
filebeat-7.1.1-x86_64.rpm
```

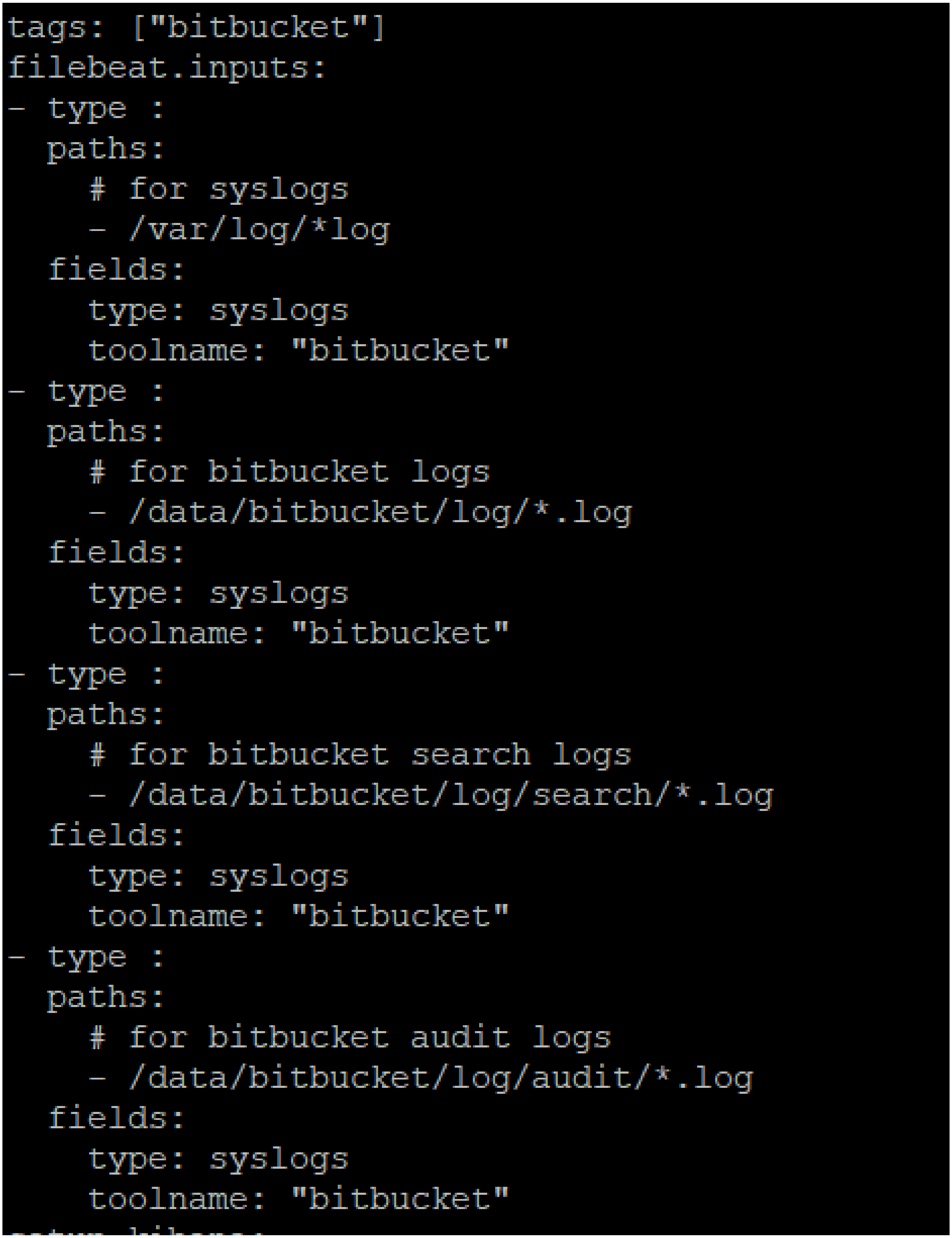
2. Edit the configuration

Modify `/etc/filebeat/filebeat.yml` to set the connection information:

```
output.elasticsearch: hosts: ["<es_url>"]

username: "elastic"

password: "<password>"

setup.kibana: host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3. Mention log files locations like below.



```
tags: ["bitbucket"]
filebeat.inputs:
- type :
  paths:
    # for syslogs
    - /var/log/*log
  fields:
    type: syslogs
    toolname: "bitbucket"
- type :
  paths:
    # for bitbucket logs
    - /data/bitbucket/log/*.log
  fields:
    type: syslogs
    toolname: "bitbucket"
- type :
  paths:
    # for bitbucket search logs
    - /data/bitbucket/log/search/*.log
  fields:
    type: syslogs
    toolname: "bitbucket"
- type :
  paths:
    # for bitbucket audit logs
    - /data/bitbucket/log/audit/*.log
  fields:
    type: syslogs
    toolname: "bitbucket"
setup.kibana:
```

4. Enable and configure the system module

```
sudo filebeat modules enable system
```

to check list of available module execute below command.

```
sudo filebeat modules list
```

5. The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

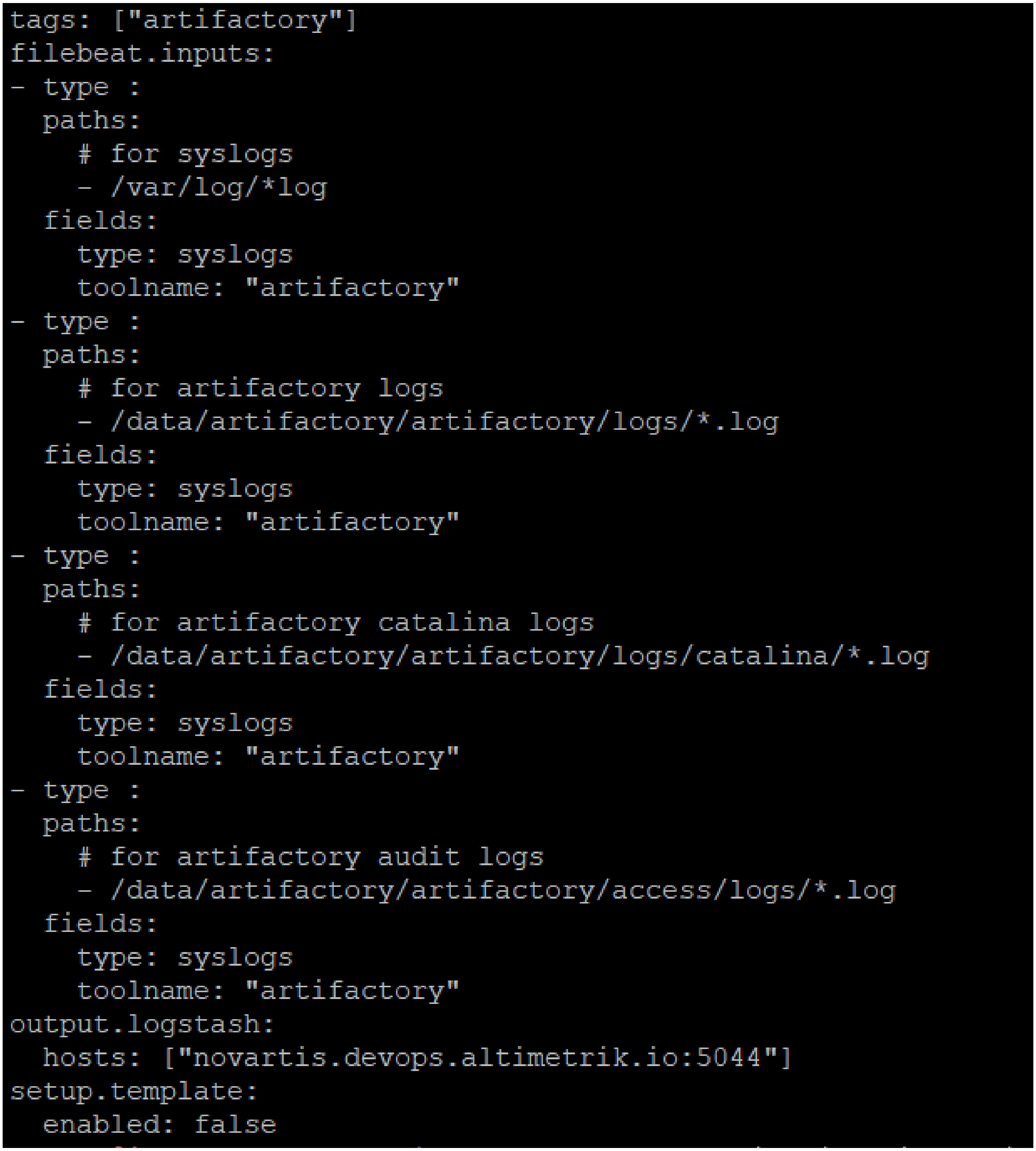
```
sudo filebeat setup
```

```
sudo service filebeat start
```

6. you can set custom index in filebeat.yml file

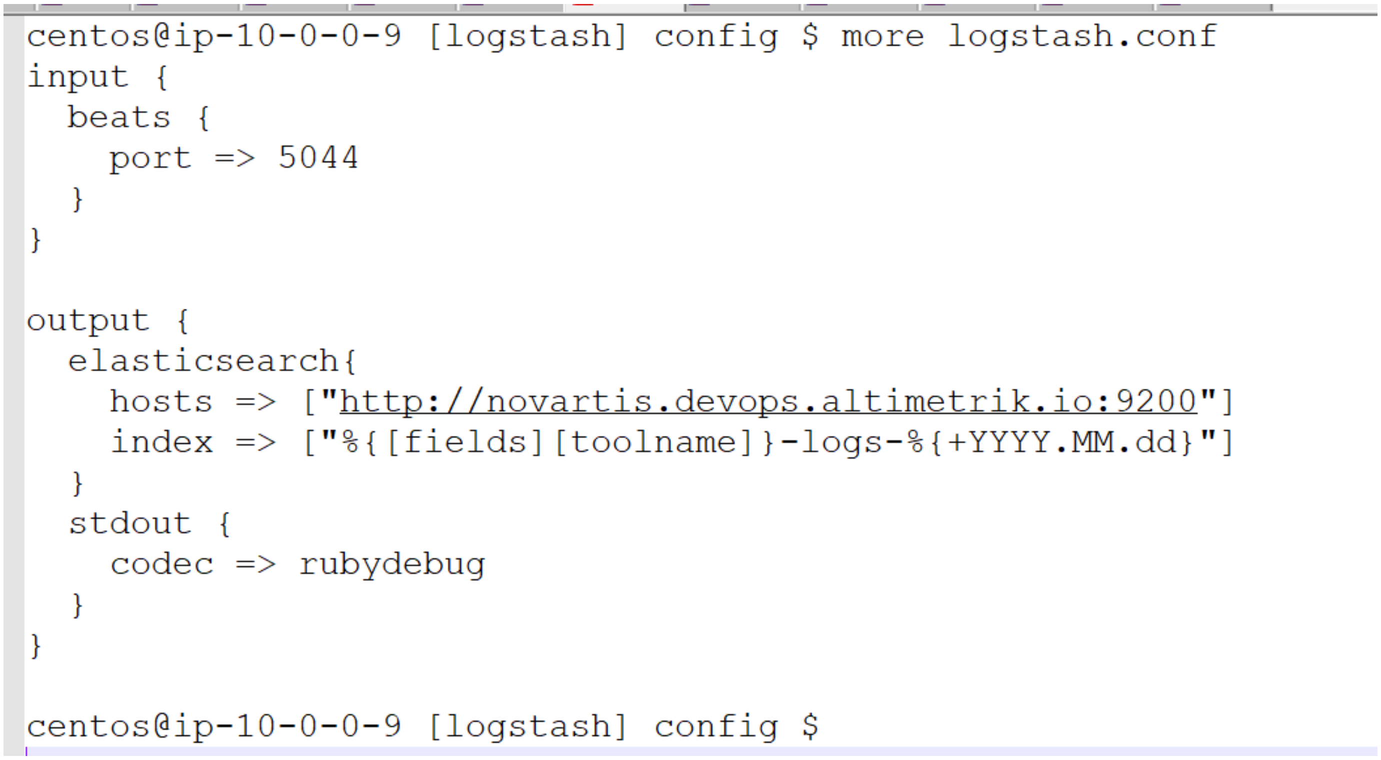
setup.dashboards.index: "bitbucket-*"

Sample filebeat file to collect log files



```
tags: ["artifactory"]
filebeat.inputs:
- type :
  paths:
    # for syslogs
    - /var/log/*log
  fields:
    type: syslogs
    toolname: "artifactory"
- type :
  paths:
    # for artifactory logs
    - /data/artifactory/artifactory/logs/*.log
  fields:
    type: syslogs
    toolname: "artifactory"
- type :
  paths:
    # for artifactory catalina logs
    - /data/artifactory/artifactory/logs/catalina/*.log
  fields:
    type: syslogs
    toolname: "artifactory"
- type :
  paths:
    # for artifactory audit logs
    - /data/artifactory/artifactory/access/logs/*.log
  fields:
    type: syslogs
    toolname: "artifactory"
output.logstash:
  hosts: ["novartis.devops.altimetrik.io:5044"]
setup.template:
  enabled: false
```

Logstash configuration to create indexes.



```
centos@ip-10-0-0-9 [logstash] config $ more logstash.conf
input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch{
    hosts => ["http://novartis.devops.altimetrik.io:9200"]
    index => ["%{[fields][toolname]}-logs-%{+YYYY.MM.dd}"]
  }
  stdout {
    codec => rubydebug
  }
}

centos@ip-10-0-0-9 [logstash] config $
```