Ketan Bhadoriya Follow
Feb 13, 2020 · 2 min read · Listen

How to create a custom index name in Filebeat

****Summary***: Filebeat creates index in default pattern: "filebeat-%{[agent.version]}-%{+yyyy.MM.dd}" -> For example: filebeat-6.7.1–2020.02.11. You can follow the steps mentioned in this article, to have your own custom index name while pushing data from Filebeat to Elasticsearch. Note: I have used Filebeat to push data directly to AWS Elasticsearch.*

1. Install the filebeat on an AWS EC2 Linux Instance using following steps:

    a. Installing Filebeat:

        1. cd /home/ec2-user
        2. curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-oss-6.7.1-x86_64.rpm
        3. sudo rpm -i filebeat-oss-6.7.1-x86_64.rpm
        4. sudo service filebeat start

2. Configure Filebeat by making following changes to filebeat.yml file stored at /etc/filebeat/filebeat.yml:

   a. Make following change in section '=== Filebeat inputs ===' (Note: In path section, I have provided apache logs path):

```
filebeat.inputs:

- type: log

# Change to true to enable this input configuration.
  enabled: true

# Paths that should be crawled and fetched. Glob based paths.
 paths:
  - /var/log/httpd/access_log
  #- c:\programdata\elasticsearch\logs\*
```

   b. Add 'setup.template.name' and 'setup.template.pattern' above 'setup.template.settings:' in section '=== Elasticsearch template setting ===' as given below (***Note*** - If you do not set up this you will get an error with regard to that) :

```
setup.template.name: "<put_custom_index_name_here>"
setup.template.pattern: "<put_custom_index_name_here>-*"

setup.template.settings:
  index.number_of_shards: 3
  #index.codec: best_compression
  #_source.enabled: false
```

  c. Change 'Elasticsearch output' which is present under '=== Outputs===' section in following way:

```
  #----------------------------- Elasticsearch output ------
  output.elasticsearch:
  # Array of hosts to connect to.
     hosts: ["<put_your_AWS-ES_endpoint_here>:443"]
     index: "<put_custom_index_name_here>-%{+yyyy.MM.dd}"
```

3. Restart the Filebeat service after making the changes mentioned above to Filebeat.yml file:

  a. sudo service filebeat restart

4. Verify whether the custom index generated using following curl command:

  a. curl -XGET '<put_your_AWS-ES_endpoint_here>/_cat/indices?pretty'

In output of above command, you should get index name in format: "<custom index name>-%{+yyyy.MM.dd}"

****Important***: Please note when you create index using filebeat the Filebeat uses time series indices (Index name contains: %{+yyyy.MM.dd}), if you do not specify time series parameter in your custom index creation as given below:*

. index: "<put_custom_index_name_here>-%{+yyyy.MM.dd}"

and you set your custom index as: . index: "<put_custom_index_name_here>"

It will take default number of shards instead of taking number of shards from 'Elasticsearch template setting' section of filebeat.yml file where 'index.number_of_shards' can be specified.