

filebeat+logstash做CDN的ncache日志采集

0、环境说明：

环境搭建：<https://download.zhoufengjie.cn/document/loganalysis/elasticsearch-logstash-kibana-install.pdf>

filebeat+logstash做CDN的ncache日志采集上传到elasticsearch，通过kibana查看。

filebeat设备ip地址：192.168.0.108

logstash设备ip地址：192.168.0.108

elasticsearch设备ip地址：192.168.0.97

kibana设备ip地址：192.168.0.97

nginx的配置文件log格式定义为：

####

```
log_format filebeat_log '$msec $request_time $remote_addr $upstream_cache_status $status  
$body_bytes_sent $request_method $scheme $host $uri $args $remote_user $upstream_addr  
$upstream_status $upstream_response_time "$upstream_http_content_type' "$http_referer"  
"$http_user_agent" "$http_cookie";
```

```
access_log /var/log/nginx/access.log filebeat_log;
```

####

1、filebeat部署：

编辑vi /etc/filebeat/filebeat.yml输入以下内容：

####

```
filebeat.inputs:  
- input_type: log  
  paths:  
    - /var/log/nginx/access*.log  
  exclude_files: ['.gz$']  
  tags: ["filebeat-nginx-accesslog"]  
  document_type: nginxaccess  
- input_type: log  
  paths:  
    - /var/log/nginx/error*.log  
  tags: ["filebeat-nginx-errorlog"]  
  exclude_files: ['.gz$']  
  document_type: nginxerror  
  tags: ["filebeat-nginx-logs"]  
  
filebeat.config.modules:  
  path: ${path.config}/modules.d/*.yml  
  reload.enabled: false  
  
output.logstash:  
  hosts: ["127.0.0.1:5044"]  
  
#output:  
## console:  
## pretty: true
```

####

临时测试【测试的时候，可以把output改成console，然后看输出】

```
/usr/bin/filebeat -e -c /etc/filebeat/filebeat.yml
```



```

}
}

output {
  if "filebeat-nginx-logs" in [tags] {
    if [logtype] == "nginxLogs" {
      elasticsearch {
        hosts => ["192.168.0.97:9200"]
        manage_template => false
        index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
      }
      #stdout {
        # codec => rubydebug
      }
    }
  }
}
}

```

####

重启logstash:

systemctl restart logstash

```

[me@logstash ~]$ systemctl restart logstash
tail -f /var/log/logstash/logstash-plain.log
[2020-05-24T17:42:47.682][INFO] [Logstash.runner] Starting Logstash ("logstash.version">7.7.0)
[2020-05-24T17:42:52.482][INFO] [org.elasticsearch.Reflections] Reflections took 57 ms to scan 1 urls, producing 21 keys and 41 values
[2020-05-24T17:42:53.677][INFO] [Logstash.outputs.elasticsearch][main] Elasticsearch pool URLs updated (changes=>[removed=>[]], added=>[http://192.168.0.97:9200/])
[2020-05-24T17:42:54.160][WARN] [Logstash.outputs.elasticsearch][main] Retained connection to ES instance (url=>http://192.168.0.97:9200/)
[2020-05-24T17:42:54.245][INFO] [Logstash.outputs.elasticsearch][main] ES Output version determined (es_version=>7)
[2020-05-24T17:42:54.255][WARN] [Logstash.outputs.elasticsearch][main] Detected a 6.x and above cluster: the 'type' event field won't be used to determine the document type (es_version=>7)
[2020-05-24T17:42:54.480][INFO] [Logstash.outputs.elasticsearch][main] New Elasticsearch output (class=>Logstash::Outputs::ElasticSearch, host=>["192.168.0.97:9200"])
[2020-05-24T17:42:55.187][INFO] [Logstash.filters.gespip][main] Using gespip database (path=>"/usr/share/logstash/vendor/bundle/ruby/2.5.0/gems/logstash-filter-geospip-6.8.3-java/vendor/GeoLite2-City.mmdb")
[2020-05-24T17:42:55.454][WARN] [org.logstash.instrument.metric.gauge.IncrefingGauge][main] A gauge metric of an unknown type (org.jruby.specialized.RubyArray$RubyObject) has been created for key: cluster_uuids. This may result in invalid serializa
ion. It is recommended to log an issue to the responsible developer/development team.
[2020-05-24T17:42:55.423][INFO] [Logstash.jvmspipeline][main] Starting pipeline (pipeline_id=>"main", "pipeline.workers">24, "pipeline.batch.size">125, "pipeline.batch.delay">50, "pipeline.max_inflight">3000, "pipeline.sources">["/etc/logstash
.conf.d/logstash.conf"], threads=>4 threads (total=>64 run)
[2020-05-24T17:42:57.659][INFO] [Logstash.inputs.beats][main] Beats inputs: Starting input listener (address=>"127.0.0.1:5044")
[2020-05-24T17:42:57.997][INFO] [Logstash.jvmspipeline][main] Pipeline started ("pipeline.id">"main")
[2020-05-24T17:42:58.055][INFO] [Logstash.agent][main] Pipelines running (count=>1, running_pipelines=>[main], non_running_pipelines=>[])
[2020-05-24T17:42:58.865][INFO] [org.logstash.beats.Server][main][afbc7f6d78384ac7ae7ae5f9d7f888877ec844a50837b789ec55d8a15b7597c] Starting server on port: 5044
[2020-05-24T17:42:58.440][INFO] [Logstash.agent][main] Successfully started logstash API endpoint (port=>5044)

```

3、查看kibana日志

管理=>索引模式=>创建索引模式=>filebeat*

管理 / 索引模式 / 创建索引模式

创建 索引模式

Kibana 使用索引模式从 Elasticsearch 索引中检索数据，以实现诸如可视化等功能。

☐ 包括系统索引

第 1 步 (共 2 步)：定义索引模式

索引模式

filebeat*

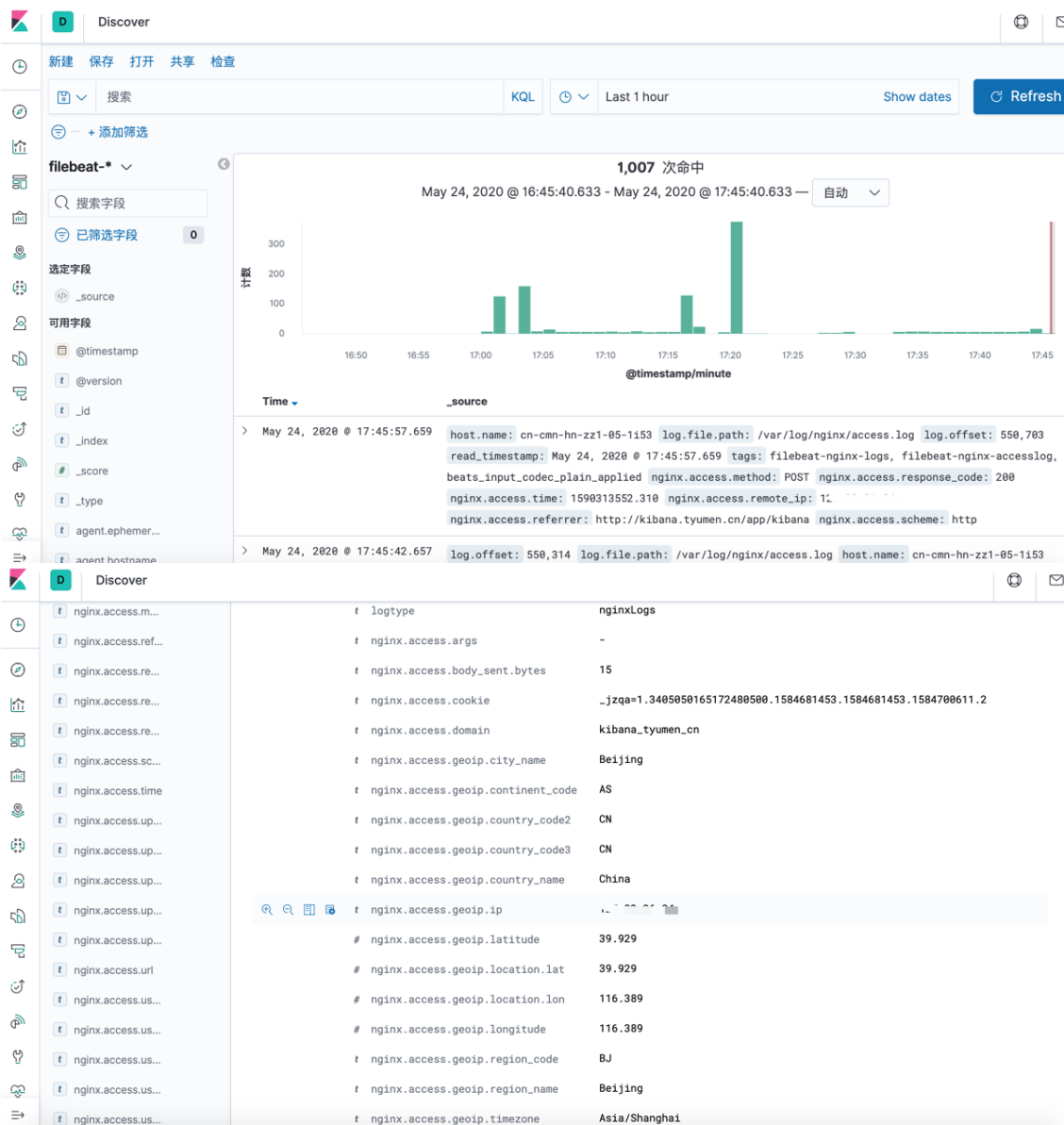
可以在索引模式中将 * 用作通配符。
不能使用空格或字符 \, /, ?, *, <, >, |。

成功! 您的索引模式匹配 1 个索引。

filebeat-7.7.0-2020.05.24

每页行数: 10

然后就可以进一步分析查看了，点击discover可以查看日志状态。



上传到elasticsearch上面的日志，通过kibana查看出来的格式如下：

```
{
  "_index": "filebeat-7.7.0-2020.05.24",
  "_type": "_doc",
  "_id": "hbWTRnIBvMHPzEOK43k7",
  "_version": 1,
  "_score": null,
  "_source": {
    "log": {
      "offset": 553424,
      "file": {
        "path": "/var/log/nginx/access.log"
      }
    },
    "host": {
      "name": "cn-cmn-hn-zz1-05-1153"
    },
    "read_timestamp": "2020-05-24T09:46:46.666Z",
    "tags": [
      "filebeat-nginx-logs",
      "filebeat-nginx-accesslog",
      "beats_input_codec_plain_applied"
    ],
    "nginx": {
      "access": {
        "method": "POST",
        "response_code": "200",
        "time": "1590313604.749",
        "remote_ip": "125.34.23.95",
        "referrer": "http://kibana.tyumen.cn/app/kibana",
        "scheme": "http",
        "user_agent": {
          "name": "Chrome",
          "os": "Mac OS X",
```

```

      "os_name": "Mac OS X",
      "os_minor": "15",
      "major": "81",
      "os_major": "10",
      "device": "Other",
      "minor": "0",
      "build": "",
      "patch": "4044"
    },
    "cookie": "_jzqa=1.3405050165172480500.1584681453.1584681453.1584700611.2",
    "body_sent": {
      "bytes": "15"
    },
    "url": "/api/ui_metric/report",
    "domain": "elk.test.tyumen.cn",
    "user_name": "ngaa",
    "request_time": "0.815",
    "upstream": {
      "cache_status": "-",
      "response_time": "0.798",
      "response_code": "200",
      "upstream_ip": "192.168.0.97:5601",
      "content_type": "application/json; charset=utf-8"
    },
    "args": "-",
    "geoip": {
      "country_code3": "CN",
      "region_name": "Beijing",
      "continent_code": "AS",
      "longitude": 116.3889,
      "location": {
        "lat": 39.9288,
        "lon": 116.3889
      },
      "latitude": 39.9288,
      "timezone": "Asia/Shanghai",
      "country_code2": "CN",
      "region_code": "BJ",
      "ip": "125.33.26.94",
      "country_name": "China",
      "city_name": "Beijing"
    }
  }
},
"@version": "1",
"ecs": {
  "version": "1.5.0"
},
"logtype": "nginxLogs",
"@timestamp": "2020-05-24T09:46:46.666Z",
"agent": {
  "ephemeral_id": "83799e29-f72d-47f7-979e-0776efddf80a",
  "type": "filebeat",
  "hostname": "cn-cmn-hn-zz1-05-1i53",
  "id": "39d4d5cf-f746-4cd8-b4ed-3c1d63d64edd",
  "version": "7.7.0"
},
"api": "/api/ui_metric/report"
},
"fields": {
  "read_timestamp": [
    "2020-05-24T09:46:46.666Z"
  ],
  "@timestamp": [
    "2020-05-24T09:46:46.666Z"
  ]
},
"sort": [
  1590313606666
]
}

```