Lesson 05 Demo 04

Configuring Filebeat to Collect Logs from Applications and Systems

Objective: To implement Filebeat for collecting server metrics and storing them in Elasticsearch for enhanced monitoring and analysis

Tools required: Filebeat

Prerequisites: None

Steps to be followed:

1. Configure Filebeat to collect logs

Step 1: Configure Filebeat to collect logs

1.1 Navigate to the terminal and update Ubuntu packages using the following commands:

sudo su

apt update

1.2 Install Java runtime using the following command:
apt -y install default-jre

```
root@ip-172-31-43-84:~# apt -y install default-jre
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  default-jre-headless
The following NEW packages will be installed:
  default-jre default-jre-headless
0 upgraded, 2 newly installed, 0 to remove and 267 not upgraded.
Need to get 3938 B of archives.
After this operation, 26.6 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 default-jre-headless amd64 2:1.11-72build2 [3042 B]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 default-jre amd64 2:1.11-72build2 [896 B]
Fetched 3938 B in 0s (222 kB/s)
Selecting previously unselected package default-jre-headless.
(Reading database ... 50%
```

1.3 Add the Elasticsearch signing key using the following command:
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

```
root@ip-172-31-24-171:/home/labuser# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasti
csearch-keyring.gpg
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) y
root@ip-172-31-24-171:/home/labuser#
```

Note: If the command displays an error indicating that the file already exists, type **y** and press the **enter** key to proceed with overwriting the existing file.

1.4 Add the repository using the following command:
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

```
root@ip-172-31-24-171:/home/labuser# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/ap
t stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
root@ip-172-31-24-171:/home/labuser#
```

1.5 Update the system packages using the following command:
apt update

```
root@ip-172-31-24-171:/home/labuser# apt update

Ign:1 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:2 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:3 https://apt.grafana.com stable InRelease
Hit:4 https://pkg.jenkins.io/debian-stable binary/ Release
Hit:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:6 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:7 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease
Hit:8 http://ap-south-1c.clouds.ports.ubuntu.com/ubuntu-ports jammy InRelease
Hit:10 http://ap-south-1c.clouds.ports.ubuntu.com/ubuntu-ports jammy-updates InRelease
Hit:11 http://ap-south-1c.clouds.ports.ubuntu.com/ubuntu-ports jammy-backports InRelease
Hit:9 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.30/deb  InRelease
Hit:13 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy InRelease
Hit:14 https://repo.zabbix.com/zabbix/6.3/ubuntu jammy InRelease
Hit:15 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu jammy InRelease
Hit:16 https://ppa.launchpadcontent.net/pipewire-debian/pipewire-upstream/ubuntu jammy InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
152 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://download.docker.com/linux/ubuntu/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
N: Skipping acquire of configured file 'main/binary-arm64/Packages' as repository 'https://repo.zabbix.com/zabbix/6.3/ubuntu jammy InRelease' doesn't support architecture 'arm64'
root@ip-172-31-24-171:/home/labuser#
```

1.6 Install Filebeat using the following command:
apt -y install filebeat

```
root@ip-172-31-43-84:~# apt -y install filebeat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 267 not upgraded.
Need to get 54.6 MB of archives.
After this operation, 201 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 filebeat amd64 8.15.1 [54.6 MB]
Fetched 54.6 MB in 1s (58.0 MB/s)
Selecting previously unselected package filebeat.
(Reading database ... 332039 files and directories currently installed.)
Preparing to unpack .../filebeat_8.15.1_amd64.deb ...
Unpacking filebeat (8.15.1) ...
Setting up filebeat (8.15.1) ...
Scanning processes...
Scanning linux images...
```

1.7 Open the Filebeat file using the following command:
sudo nano /etc/filebeat/filebeat.yml

```
root@ip-172-31-24-171:/home/labuser# sudo nano /etc/filebeat/filebeat.yml
```

1.8 Comment on the following lines in the **Elasticsearch Output** section:

#output.elasticsearch:

 # Array of hosts to connect to.

 # hosts: [“localhost:9200”]

```
# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
 #hosts: ["localhost:9200"]
```

1.9 Uncomment the following lines in the **Logstash Output** section:

output.logstash:

hosts: [“localhost:5044”]

```
# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
#  hosts: ["localhost:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
 # preset: balanced

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"
```

1.10 View the list of available modules using the following command:

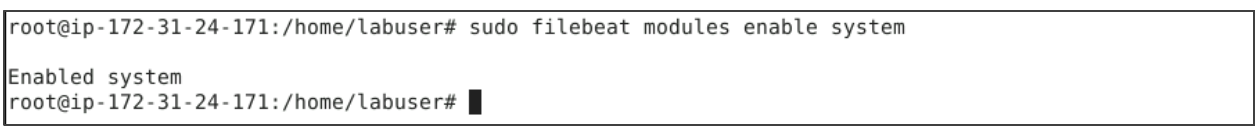
filebeat modules list

```
root@ip-172-31-36-251:~# filebeat modules list
Enabled:

Disabled:
activemq
apache
auditd
aws
awsfargate
azure
cef
checkpoint
cisco
coredns
crowdstrike
cyberarkpas
elasticsearch
envoyproxy
fortinet
gcp
```

1.11 Enable the Filebeat system for the modules using the following command:

sudo filebeat modules enable system

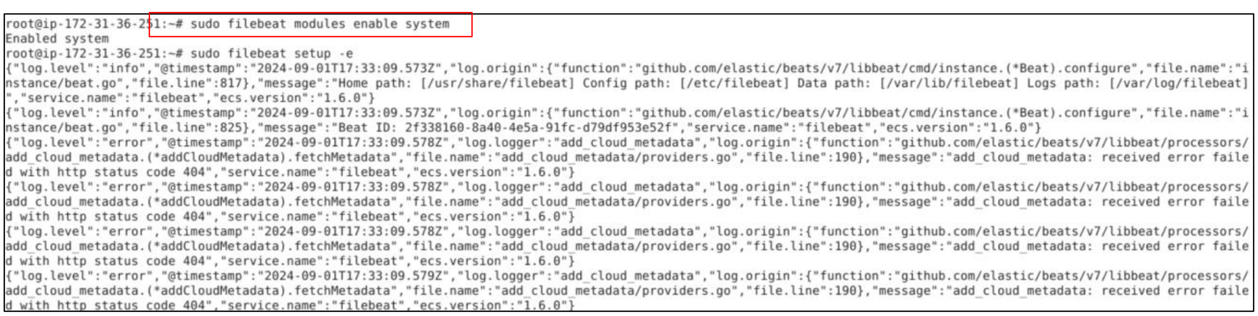


```
root@ip-172-31-24-171:/home/labuser# sudo filebeat modules enable system

Enabled system
root@ip-172-31-24-171:/home/labuser#
```

1.12 After installing the modules in Filebeat, proceed with the following command:

sudo filebeat setup -e



```
root@ip-172-31-36-251:~# sudo filebeat modules enable system
Enabled system
root@ip-172-31-36-251:~# sudo filebeat setup -e
```


```
{"log.level":"info","@timestamp":"2024-09-01T17:33:09.573Z","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).configure","file.name":"i
nstance/beat.go","file.line":817},"message":"Home path: [/usr/share/filebeat] Config path: [/etc/filebeat] Data path: [/var/lib/filebeat] Logs path: [/var/log/filebeat]
","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-09-01T17:33:09.573Z","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).configure","file.name":"i
nstance/beat.go","file.line":825},"message":"Beat ID: 2f338160-8a40-4e5a-91fc-d79df953e52f","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2024-09-01T17:33:09.578Z","log.logger":"add_cloud_metadata","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/processors/
add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"add_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error faile
d with http status code 404","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2024-09-01T17:33:09.578Z","log.logger":"add_cloud_metadata","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/processors/
add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"add_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error faile
d with http status code 404","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2024-09-01T17:33:09.578Z","log.logger":"add_cloud_metadata","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/processors/
add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"add_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error faile
d with http status code 404","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2024-09-01T17:33:09.579Z","log.logger":"add_cloud_metadata","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/processors/
add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"add_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error faile
d with http status code 404","service.name":"filebeat","ecs.version":"1.6.0"}
```

1.13 Execute the following command to start, enable, and check the status of the Filebeat service:

sudo systemctl start filebeat

sudo systemctl enable filebeat

sudo systemctl status filebeat

```
root@ip-172-31-43-84:~# sudo systemctl start filebeat
root@ip-172-31-43-84:~#
root@ip-172-31-43-84:~# sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
root@ip-172-31-43-84:~#
root@ip-172-31-43-84:~# sudo systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-09-12 16:44:39 UTC; 14s ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 13336 (filebeat)
      Tasks: 9 (limit: 18808)
     Memory: 36.8M
        CPU: 110ms
     CGroup: /system.slice/filebeat.service
             └─13336 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat

Sep 12 16:44:39 ip-172-31-43-84 systemd[1]: Started Filebeat sends log files to Logstash or directly to Elasticsearch..
root@ip-172-31-43-84:~#
```

1.14 Verify if Elasticsearch is receiving the Filebeat data log using the following command:

curl -XGET http://localhost:9200/_cat/indices?v

```
root@ip-172-31-36-251:~# curl -XGET http://localhost:9200/_cat/indices?v
health status index                                                                uuid                   pri rep docs.count docs.deleted store.size pri.store.size datase
t.size
green  open   .internal.alerts-transform.health.alerts-default-000001             akyPPSTtTdWJQ7iz_yIBlA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.logs.alerts-default-000001           C1HbQ-ZyROybsXzvkHU4GA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.uptime.alerts-default-000001         aGuDK6DYRTiH3B2RdtbOSA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-ml.anomaly-detection.alerts-default-000001        BKA5DCFKTRGbchEoBSDWpA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.slo.alerts-default-000001           LkBMzdHxRQG67qozmAb5cA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-default.alerts-default-000001                     F2OhckcfS2umFtfJLYnYgw   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.apm.alerts-default-000001           3re6SAPwS9WIq3B5tuch2w   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.metrics.alerts-default-000001       zriLItdESjeRB_gt32DNQw   1   0          0            0       249b           249b
  249b
green  open   .kibana-observability-ai-assistant-conversations-000001           4g_ETc0KT5OV17Rn1w_2Pw   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 bxF5ZWk-RR-jOKEjzcnsNA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-observability.threshold.alerts-default-000001     Z4psvNawScKsUR-Ak1MqOw   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-security.alerts-default-000001                    59tQt_aqSjKbAMtKPu2oqA   1   0          0            0       249b           249b
  249b
green  open   .kibana-observability-ai-assistant-kb-000001                       XqGa2LcmT1WI9982md-JzA   1   0          0            0       249b           249b
  249b
green  open   .internal.alerts-stack.alerts-default-000001                       kkWjXyL0S0qFZi9GfXRqsA   1   0          0            0       249b           249b
  249b
root@ip-172-31-36-251:~#
```

By following these steps, you have successfully configured Filebeat to collect and store server metrics in Elasticsearch, enhancing your system's monitoring capabilities.