Lesson 05 Demo 05

Building an Automated Log Processing Pipeline with Kafka and ELK Stack

Objective: To integrate Kafka with ELK Stack to buffer and process log surges, protecting Logstash and Elasticsearch during high-volume events for improved reliability and scalable log management

Tools required: ELK Stack and Kafka

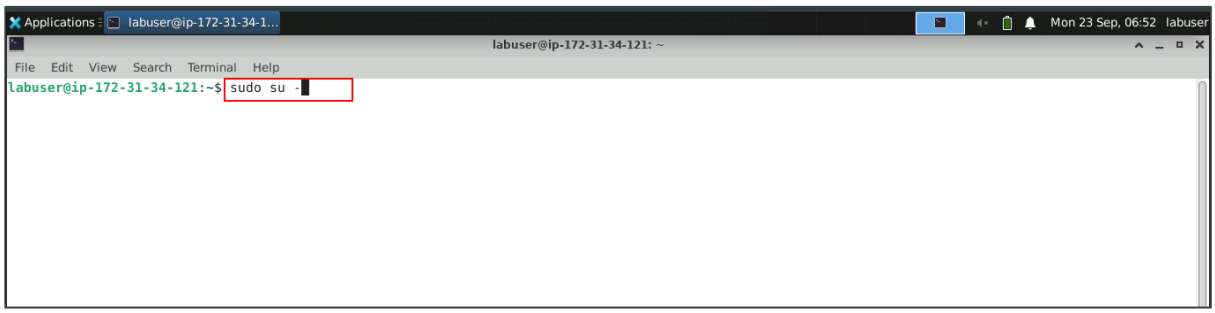
Prerequisites: None

Steps to be followed:

1. Set up the system and install Java Runtime Environment (JRE)
2. Set up the Apache Kafka message broker
3. Create a topic for the Apache logs

Step 1: Set up the system and install Java Runtime Environment (JRE)

1.1 Run the following commands in the Ubuntu lab to log in as the root user, gain admin access, and update Ubuntu packages:
sudo su -
apt update



```
Applications  root@ip-172-31-34-121: ~                                  Mon 23 Sep, 06:54  labuser
root@ip-172-31-34-121: ~
File  Edit  View  Search  Terminal  Help
labuser@ip-172-31-34-121:~$ sudo su -
root@ip-172-31-34-121:~#
root@ip-172-31-34-121:~#
root@ip-172-31-34-121:~# apt update
```

```
Applications  root@ip-172-31-34-121: ~                                  Mon 23 Sep, 06:54  labuser
root@ip-172-31-34-121: ~
File  Edit  View  Search  Terminal  Help
labuser@ip-172-31-34-121:~$ sudo su -
root@ip-172-31-34-121:~#
root@ip-172-31-34-121:~#
root@ip-172-31-34-121:~# apt update
Hit:1 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy InRelease
Hit:2 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-updates InRelease
Hit:3 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-backports InRelease
Hit:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:5 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:6 https://download.docker.com/linux/ubuntu jammy InRelease
Ign:7 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:8 https://apt.grafana.com stable InRelease
Hit:9 https://pkg.jenkins.io/debian-stable binary/ Release
Get:11 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease [129 kB]
Hit:10 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.30/deb  InRelease
Hit:12 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu jammy InRelease
Hit:13 https://ppa.launchpadcontent.net/pipewire-debian/pipewire-upstream/ubuntu jammy InRelease
Fetched 129 kB in 2s (67.7 kB/s)
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://artifacts.elastic.co/packages/8.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the
DEPRECATION section in apt-key(8) for details.
W: https://download.docker.com/linux/ubuntu/dists/jammy/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPREC
ATION section in apt-key(8) for details.
root@ip-172-31-34-121:~#
```

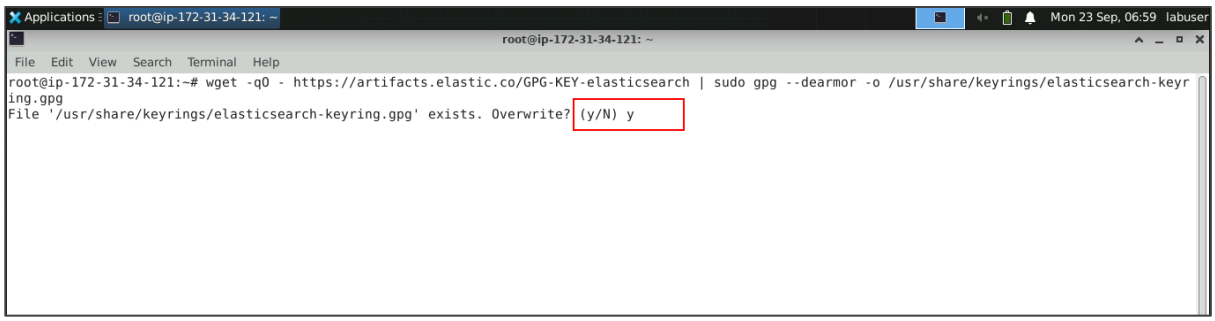
1.2 Execute the following command to install JRE, which Filebeat will use:

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%
```

After JRE is installed, proceed with the installation of the Elasticsearch component of ELK Stack. To do this, add the signing key and repositories to the system first.

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



> **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 Run the following command to add the repository in **/etc/apt/sources.list.d/elastic-8.x.list**:
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

1.5 Run following command to update the system packages:

apt update

```
root@ip-172-31-36-251:~#
root@ip-172-31-36-251:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
root@ip-172-31-36-251:~#
root@ip-172-31-36-251:~# 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
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
root@ip-172-31-36-251:~#
root@ip-172-31-36-251:~# apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10.4 kB]
Hit:5 https://download.docker.com/linux/ubuntu jammy InRelease
Ign:6 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:7 https://pkg.jenkins.io/debian-stable binary/ Release
Hit:9 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:8 https://prod-cdn.packages.k8s.io/repositories/isv:/kubernetes:/core:/stable:/v1.28/deb  InRelease
Get:10 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [109 kB]
Fetched 109 kB in 1s (155 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
256 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Ignoring file 'elastic-8.x.listecho' in directory '/etc/apt/sources.list.d/' as it has an invalid filename extension
root@ip-172-31-36-251:~#
```

1.6 Run the following command to configure a Logstash pipeline that pulls logs from a Kafka topic, processes them, and ships them to Elasticsearch for indexing:

vim /etc/logstash/conf.d/apache.conf

```
Applications  root@ip-172-31-34-121: ~                                  Mon 23 Sep, 07:03  labuser
root@ip-172-31-34-121: ~
File  Edit  View  Search  Terminal  Help
root@ip-172-31-34-121:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyr
ing.gpg
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) y
root@ip-172-31-34-121:~# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable mai
n" | 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-172-31-34-121:~# apt update
Hit:1 https://apt.grafana.com stable InRelease
Hit:2 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:3 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy InRelease
Hit:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Ign:5 https://pkg.jenkins.io/debian-stable binary/ InRelease
Hit:6 https://pkg.jenkins.io/debian-stable binary/ Release
Hit:7 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:8 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-updates InRelease
Get:10 http://ports.ubuntu.com/ubuntu-ports jammy-security InRelease [129 kB]
Hit:11 http://us-east-1.ec2.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:12 https://ppa.launchpadcontent.net/ansible/ansible/ubuntu jammy InRelease
Hit:13 https://ppa.launchpadcontent.net/pipewire-debian/pipewire-upstream/ubuntu jammy InRelease
Fetched 129 kB in 2s (69.7 kB/s)
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 DEPREC
ATION section in apt-key(8) for details.
root@ip-172-31-34-121:~# vim /etc/logstash/conf.d/apache.conf
```

1.7 Copy and paste the following configurations

```
input {
  kafka {
    bootstrap_servers => "localhost:9092"
    topics => "apache"
    }
}
filter {
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
    date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
    }
  geoip {
      source => "source_ip"
      target => "source_geo"
   }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "logstash"
  }
}
```

```
root@ip-172-31-43-84:~# vim /etc/logstash/conf.d/apache.conf
root@ip-172-31-43-84:~# cat /etc/logstash/conf.d/apache.conf
input {
  kafka {
    bootstrap_servers => "localhost:9092"
    topics => "apache"
    }
}
filter {
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
    date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
    }
  geoip {
      source => "source_ip"
      target => "source_geo"
   }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "logstash"
  }
}

root@ip-172-31-43-84:~#
```

1.8 Execute the following commands to install the Apache package:

apt install -y apache2

service apache2 start

service apache2 status

```
root@ip-172-31-43-84:~# apt install -y apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0
0 upgraded, 9 newly installed, 0 to remove and 267 not upgraded.
Need to get 2062 kB of archives.
After this operation, 8234 kB of additional disk space will be used.
```

```
root@ip-172-31-43-84:~# service apache2 start
root@ip-172-31-43-84:~#
root@ip-172-31-43-84:~# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-09-12 16:50:14 UTC; 29s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 15081 (apache2)
      Tasks: 55 (limit: 18808)
     Memory: 5.3M
        CPU: 35ms
     CGroup: /system.slice/apache2.service
             ├─15081 /usr/sbin/apache2 -k start
             ├─15083 /usr/sbin/apache2 -k start
             └─15084 /usr/sbin/apache2 -k start

Sep 12 16:50:14 ip-172-31-43-84 systemd[1]: Starting The Apache HTTP Server...
Sep 12 16:50:14 ip-172-31-43-84 systemd[1]: Started The Apache HTTP Server.
root@ip-172-31-43-84:~#
```

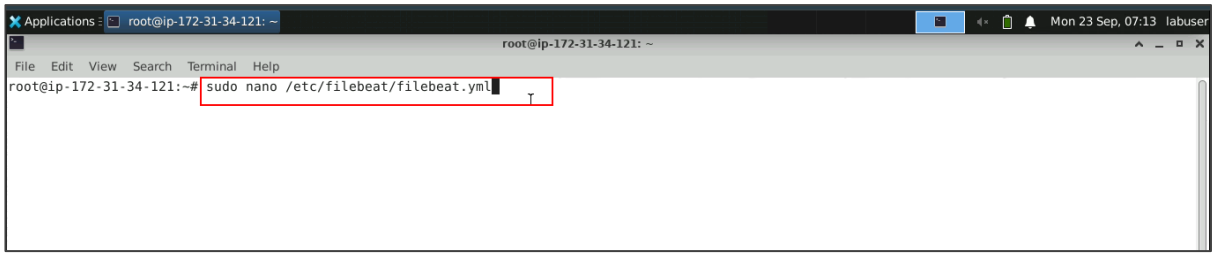
1.9 Execute the following command to install the Filebeat package:

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...
```

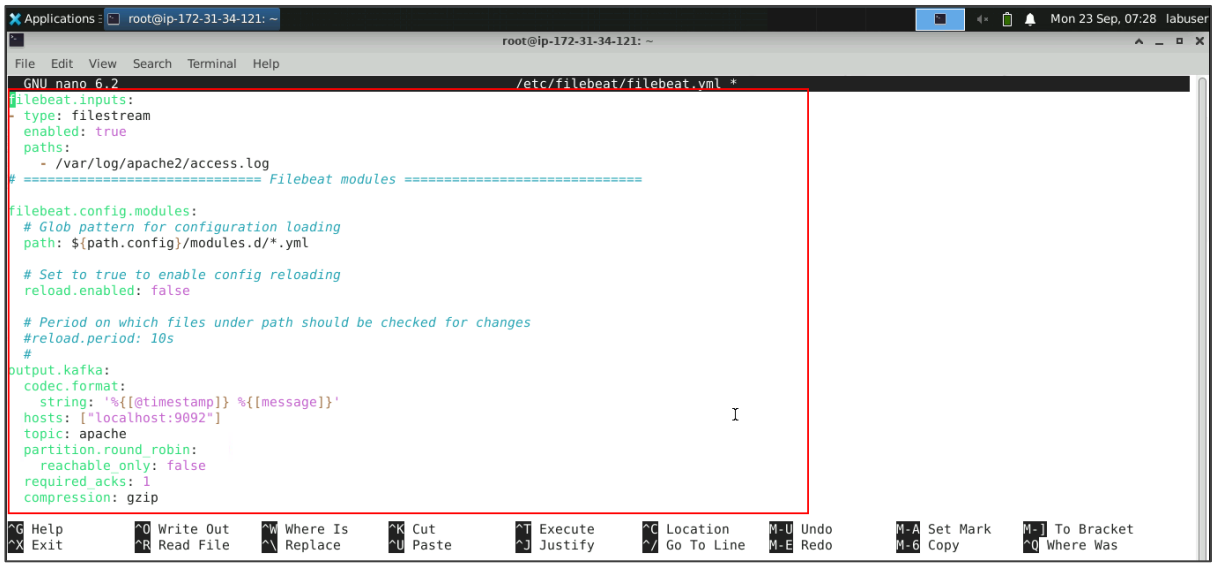
1.10 Run the command below to modify Filebeat so it can send logs to Logstash:

sudo nano /etc/filebeat/filebeat.yml



1.11 Update the **YAML** file using the following script:

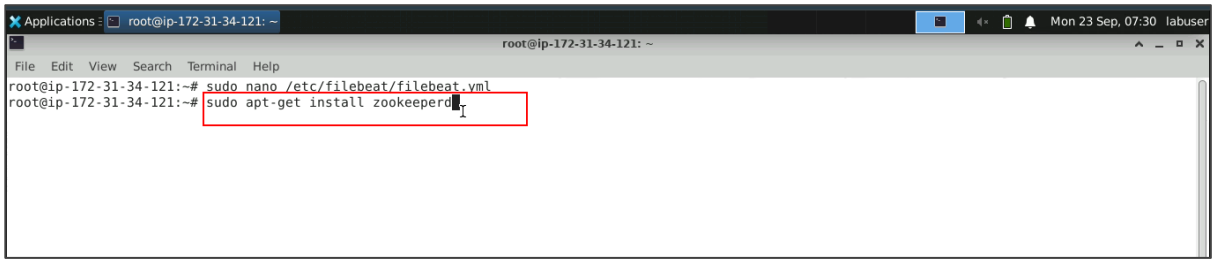
```
filebeat.inputs:
- type: filestream
  enabled: true
  paths:
    - /var/log/apache2/access.log
# ============================== Filebeat modules
==============================

filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yml

  # Set to true to enable config reloading
  reload.enabled: false

  # Period on which files under path should be checked for changes
  #reload.period: 10s
  #
output.kafka:
  codec.format:
    string: '%{[@timestamp]} %{[message]}'
  hosts: ["localhost:9092"]
  topic: apache
  partition.round_robin:
    reachable_only: false
  required_acks: 1
  compression: gzip
  max_message_bytes: 1000000
```



Step 2: Set up the Apache Kafka message broker

2.1 Execute the following command to install and set up the Apache Kafka message broker:

sudo apt-get install zookeeperd



Note: Kafka uses ZooKeeper to maintain configuration information and synchronization.

```
root@ip-172-31-34-121:~# sudo nano /etc/filebeat/filebeat.yml
root@ip-172-31-34-121:~# sudo apt-get install zookeeperd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libjline-java liblog4j1.2-java libxerces2-java libxml-commons-external-java libxml-commons-resolver1.1-java libzookeeper-java zookeeper
Suggested packages:
  libjline-java-doc liblog4j1.2-java-doc libmail-java libxerces2-java-doc libxml-commons-resolver1.1-java-doc libzookeeper-java-doc
The following NEW packages will be installed:
  libjline-java liblog4j1.2-java libxerces2-java libxml-commons-external-java libxml-commons-resolver1.1-java libzookeeper-java zookeeper
  zookeeperd
0 upgraded, 8 newly installed, 0 to remove and 152 not upgraded.
Need to get 3778 kB of archives.
After this operation, 4548 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 libjline-java all 1.0-3 [71.5 kB]
Get:2 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 liblog4j1.2-java all 1.2.17-11 [439 kB]
Get:3 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 libxml-commons-external-java all 1.4.01-5 [240 kB]
Get:4 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 libxml-commons-resolver1.1-java all 1.2-11 [97.6 kB]
Get:5 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy/universe arm64 libxerces2-java all 2.12.1-1 [1437 kB]
Get:6 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 libzookeeper-java all 3.4.13-6ubuntu4.1 [1372 kB]
Get:7 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 zookeeper all 3.4.13-6ubuntu4.1 [112 kB]
Get:8 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports jammy-updates/universe arm64 zookeeperd all 3.4.13-6ubuntu4.1 [8290 B]
Fetched 3778 kB in 3s (1408 kB/s)
```

2.2 Run the following commands to download and extract Kafka:

wget https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz

tar -xvzf kafka_2.12-3.8.0.tgz

sudo cp -r kafka_2.12-3.8.0 /opt/kafka

```
root@ip-172-31-34-121:~# wget https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz
```

```
root@ip-172-31-34-121:~# wget https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz
--2024-09-23 07:32:47--  https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz
Resolving downloads.apache.org (downloads.apache.org)... 88.99.208.237, 135.181.214.104, 2a01:4f9:3a:2c57::2, ...
Connecting to downloads.apache.org (downloads.apache.org)|88.99.208.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 120900366 (115M) [application/x-gzip]
Saving to: ‘kafka_2.12-3.8.0.tgz’

kafka_2.12-3.8.0.tgz                100%[===================================================================>] 115.30M  28.0MB/s    in 5.3s

2024-09-23 07:32:53 (21.8 MB/s) - ‘kafka_2.12-3.8.0.tgz’ saved [120900366/120900366]

root@ip-172-31-34-121:~#
```

```
root@ip-172-31-34-121:~# wget https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz
--2024-09-23 07:32:47--  https://downloads.apache.org/kafka/3.8.0/kafka_2.12-3.8.0.tgz
Resolving downloads.apache.org (downloads.apache.org)... 88.99.208.237, 135.181.214.104, 2a01:4f9:3a:2c57::2, ...
Connecting to downloads.apache.org (downloads.apache.org)|88.99.208.237|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 120900366 (115M) [application/x-gzip]
Saving to: 'kafka_2.12-3.8.0.tgz'

kafka_2.12-3.8.0.tgz                100%[===================================================================>] 115.30M  28.0MB/s    in 5.3s

2024-09-23 07:32:53 (21.8 MB/s) - 'kafka_2.12-3.8.0.tgz' saved [120900366/120900366]

root@ip-172-31-34-121:~# tar -xvzf kafka_2.12-3.8.0.tgz
```

```
root@ip-172-31-34-121:~# sudo cp -r kafka_2.12-3.8.0 /opt/kafka
```

2.3 Run the following command to start Kafka:

sudo /opt/kafka/bin/kafka-server-start.sh /opt/kafka/config/server.properties

```
root@ip-172-31-34-121:~# sudo cp -r kafka_2.12-3.8.0 /opt/kafka
root@ip-172-31-34-121:~# sudo /opt/kafka/bin/kafka-server-start.sh /opt/kafka/config/server.properties
```

You will see the following interface:

```
e may not be available. (org.apache.kafka.clients.NetworkClient)
[2024-09-02 15:31:08,034] INFO [Controller id=0, targetBrokerId=0] Client requested connection close from node 0 (org.apache.kafka.clients.NetworkClient)
[2024-09-02 15:31:08,078] INFO [/config/changes-event-process-thread]: Starting (kafka.common.ZkNodeChangeNotificationListener$ChangeEventProcessThread)
[2024-09-02 15:31:08,115] INFO [SocketServer listenerType=ZK_BROKER, nodeId=0] Enabling request processing. (kafka.network.SocketServer)
[2024-09-02 15:31:08,122] INFO Awaiting socket connections on 0.0.0.0:9092. (kafka.network.DataPlaneAcceptor)
[2024-09-02 15:31:08,158] INFO [KafkaServer id=0] Start processing authorizer futures (kafka.server.KafkaServer)
[2024-09-02 15:31:08,159] INFO [KafkaServer id=0] End processing authorizer futures (kafka.server.KafkaServer)
[2024-09-02 15:31:08,159] INFO [KafkaServer id=0] Start processing enable request processing future (kafka.server.KafkaServer)
[2024-09-02 15:31:08,160] INFO [KafkaServer id=0] End processing enable request processing future (kafka.server.KafkaServer)
[2024-09-02 15:31:08,167] INFO Kafka version: 3.8.0 (org.apache.kafka.common.utils.AppInfoParser)
[2024-09-02 15:31:08,167] INFO Kafka commitId: 771b9576b00ecf5b (org.apache.kafka.common.utils.AppInfoParser)
[2024-09-02 15:31:08,167] INFO Kafka startTimeMs: 1725291068160 (org.apache.kafka.common.utils.AppInfoParser)
[2024-09-02 15:31:08,171] INFO [KafkaServer id=0] started (kafka.server.KafkaServer)
[2024-09-02 15:31:08,283] INFO [zk-broker-0-to-controller-forwarding-channel-manager]: Recorded new ZK controller, from now on will use node ip-172-31-36-251.ec2.intern
al:9092 (id: 0 rack: null) (kafka.server.NodeToControllerRequestThread)
[2024-09-02 15:31:08,339] INFO [zk-broker-0-to-controller-alter-partition-channel-manager]: Recorded new ZK controller, from now on will use node ip-172-31-36-251.ec2.i
nternal:9092 (id: 0 rack: null) (kafka.server.NodeToControllerRequestThread)
```

Step 3: Create a topic for the Apache logs

3.1 Execute the following command in a new terminal tab to create a topic for the Apache logs:
/opt/kafka/bin/kafka-topics.sh --create --bootstrap-server localhost:9092 --replication-factor 1 --partitions 1 --topic apache

```
root@ip-172-31-36-251:~# /opt/kafka/bin/kafka-topics.sh --create --bootstrap-server localhost:9092 --replication-factor 1 --partitions 1 --topic apache
Created topic apache.
root@ip-172-31-36-251:~#
```

The **Created topic apache** message is displayed as shown below:

```
root@ip-172-31-36-251:~# /opt/kafka/bin/kafka-topics.sh --create --bootstrap-server localhost:9092 --replication-factor 1 --partitions 1 --topic apache
Created topic apache.
root@ip-172-31-36-251:~#
```

3.2 Run the commands below to start the Filebeat service, enable Filebeat at system startup, and check the status:
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:~#
```

3.3 Run the following command to verify that ElasticSearch is receiving the Filebeat data log:

curl -X GET "localhost:9200/_cat/indices?v" | grep logstash

```
root@ip-172-31-21-55:/var/log/filebeat# curl -X GET "localhost:9200/_cat/indices?v" | grep logstash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2975    0  2975    0     0   442k      0 --:--:-- --:--:-- --:--:--  484k
yellow open   logstash                                                    NakDRkMKTICd-xAaAA4gHA   1   1          3            0     20.4kb         20.4kb
20.4kb
root@ip-172-31-21-55:/var/log/filebeat#
root@ip-172-31-21-55:/var/log/filebeat#
```

The displayed output is as shown below:

```
root@ip-172-31-21-55:/var/log/filebeat# curl -X GET "localhost:9200/_cat/indices?v" | grep logstash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2975    0  2975    0     0   442k      0 --:--:-- --:--:-- --:--:--  484k
yellow open   logstash                                                    NakDRkMKTICd-xAaAA4gHA   1   1          3            0     20.4kb         20.4kb
20.4kb
root@ip-172-31-21-55:/var/log/filebeat#
root@ip-172-31-21-55:/var/log/filebeat#
```

By following these steps, you have successfully integrated Kafka with ELK Stack to buffer and process log surges, protecting Logstash and Elasticsearch during high-volume events for improved reliability and scalable log management.