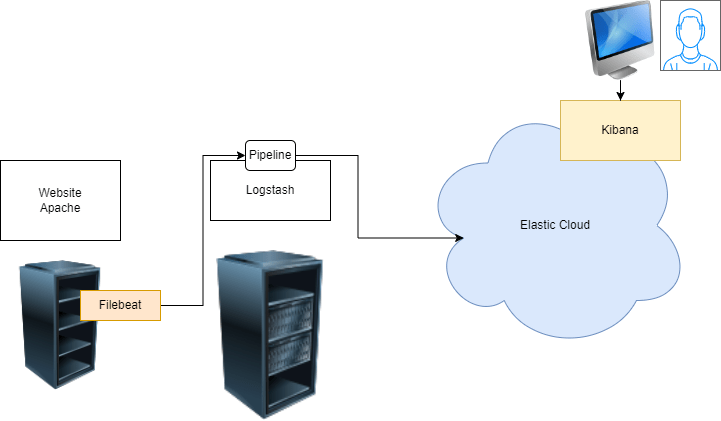
**Sending logs to elastic cloud**

* Overview  
  
* Install apache and filebeat on one linux instance <https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html>

sudo apt update

sudo apt install apache2 -y

* Install logstash on other linux instance <https://www.elastic.co/guide/en/logstash/current/installing-logstash.html>

**Configuring filebeats to send apache access logs to logstash**

* <https://www.elastic.co/guide/en/beats/filebeat/current/logstash-output.html> for basic configuration information
* Sending data from logstash to elastic cloud <https://www.elastic.co/guide/en/logstash/current/connecting-to-cloud.html>
* Logstash pipeline

input {

beats {

port => 5044

}

}

filter {

grok {

match => { "message" => "%{COMBINEDAPACHELOG}" }

}

}

output {

elasticsearch {

cloud\_id => "learningenv:dXMtY2VudHJhbDEuZ2NwLmNsb3VkLmVzLmlvOjQ0MyQxMDg1YTVjOWQyOWY0N2FjODkyNTBmNjY3NjJkYWU3MyRlNDM5MGRmYmJmMzM0MGViODZiMGNhNTg3ODA1MmZkOQ=="

cloud\_auth => "elastic:h22oWprNjqqbEGTKPSvHHpqS"

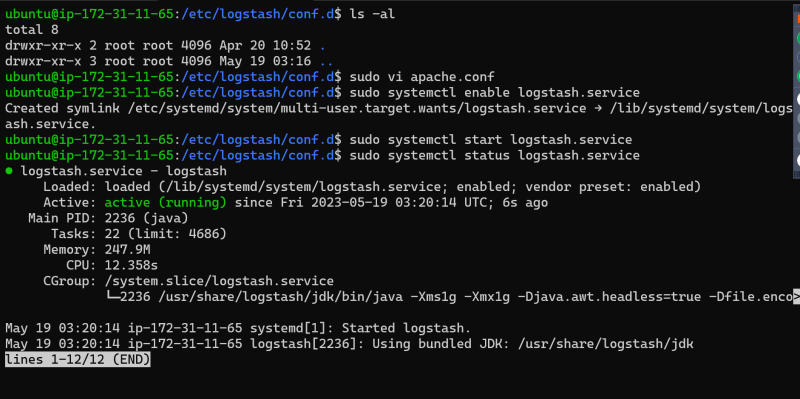
}

file {

path => /tmp/test.log

}

}

* Create a file called as apache.conf in /etc/logstash/conf.d
* Enable and start logstash service  
  
* Now configure filebeat to send logs from /var/log/apache2/access.log to logstash
* To generate artifical traffic we have executed the following script

#!/bin/bash

while true; do

curl 'http://34.219.90.251'

sleep 2

done

* As of now we are getting issue with indexing (storing ) in elastic search

[WARN ] 2023-05-19 03:52:25.065 [[main]>worker0] elasticsearch - Could not index event to Elasticsearch. status: 400, action: ["index", {:\_id=>nil, :\_index=>"apachelog-2023.05.19", :routing=>nil, :pipeline=>"apachelogs"}, {"log"=>{"offset"=>29714, "file"=>{"path"=>"/var/log/apache2/access.log"}}, "message"=>"157.48.143.223 - - [19/May/2023:03:52:15 +0000] \"-\" 408 0 \"-\" \"-\"", "@version"=>"1", "cloud"=>{"machine"=>{"type"=>"t2.medium"}, "account"=>{"id"=>"678879106782"}, "provider"=>"aws", "availability\_zone"=>"us-west-2c", "image"=>{"id"=>"ami-0fcf52bcf5db7b003"}, "region"=>"us-west-2", "service"=>{"name"=>"EC2"}, "instance"=>{"id"=>"i-0b27f5e82d459e378"}}, "source"=>{"address"=>"157.48.143.223"}, "input"=>{"type"=>"filestream"}, "timestamp"=>"19/May/2023:03:52:15 +0000", "ecs"=>{"version"=>"8.0.0"}, "http"=>{"response"=>{"status\_code"=>408, "body"=>{"bytes"=>0}}}, "@timestamp"=>2023-05-19T03:52:23.879Z, "event"=>{"original"=>"157.48.143.223 - - [19/May/2023:03:52:15 +0000] \"-\" 408 0 \"-\" \"-\""}, "host"=>{"id"=>"b9e46fc917bf4bc080ee389c0cef33ad", "name"=>"ip-172-31-10-238", "containerized"=>false, "hostname"=>"ip-172-31-10-238", "os"=>{"name"=>"Ubuntu", "codename"=>"jammy", "version"=>"22.04.2 LTS (Jammy Jellyfish)", "platform"=>"ubuntu", "kernel"=>"5.15.0-1031-aws", "type"=>"linux", "family"=>"debian"}, "architecture"=>"x86\_64", "ip"=>["172.31.10.238", "fe80::8ef:a7ff:fe5a:5c85"], "mac"=>["0A-EF-A7-5A-5C-85"]}, "tags"=>["beats\_input\_codec\_plain\_applied"], "agent"=>{"id"=>"130803ea-47c3-46d3-aad8-8ba6449baff2", "name"=>"ip-172-31-10-238", "version"=>"8.7.1", "ephemeral\_id"=>"1b68db3e-0975-4e11-a939-83d1318ed448", "type"=>"filebeat"}}], response: {"index"=>{"\_index"=>"apachelog-2023.05.19", "\_id"=>nil, "status"=>400, "error"=>{"type"=>"illegal\_argument\_exception", "reason"=>"pipeline with id [apachelogs] does not exist"}}}

[INFO ] 2023-05-19 03:52:25.066 [[main]>worker0] file - Opening file {:path=>"/tmp/test.log"