GNU nano 8.1 /etc/logstash/conf.d/beats.conf

pattern\_definitions => {

"APACHE\_TIME" => "%{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{YEAR}"

}

remove\_field => "message"

}

date {

match => [ "[apache][error][timestamp]", "EEE MMM dd H:m:s YYYY", "EEE MMM dd H:m:s.SSSSSS YYYY" ]

remove\_field => "[apache][error][timestamp]"

}

grok {

match => { "[source][address]" => ["^(%{IP:[source][ip]}|%{HOSTNAME:[source][domain]})$"]}

}

geoip {

source => "[source][ip]"

target => "[source][geo]"

}

}

}

date {

match => ["timestamp", "MMM dd HH:mm:ss"]

}

}

output {

if [@metadata][pipeline] {

elasticsearch {

ssl => true

hosts =>["https://157.230.250.174:9200"]

cacert => "/etc/logstash/certs/http\_ca.crt"

user => "logstash\_internal"

password => "123456"

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

pipeline => "%{[@metadata][pipeline]}"

}

} else {

elasticsearch {

ssl => true

hosts => ["https://157.230.250.174:9200"]

cacert => "/etc/logstash/certs/http\_ca.crt"

user => "logstash\_internal"

password => "123456"

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

}

}

}