**Apache**

Sample logs

025-03-10 14:25:43,123 INFO [order-service] - Order ID 4567 processed successfully in 120ms

2025-03-10 14:25:44,789 ERROR [payment-service] - Payment ID 8910 failed due to insufficient funds

Grok

%{TIMESTAMP\_ISO8601:log\_timestamp} %{LOGLEVEL:log\_level} \[%{DATA:service}\] - %{GREEDYDATA:message}

Logstash

filter {

grok {

match => {

"message" => [

"%{IPORHOST:client\_ip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] \"%{WORD:method} %{URIPATHPARAM:request} HTTP/%{NUMBER:http\_version}\" %{NUMBER:response\_code} %{NUMBER:bytes}",

"%{TIMESTAMP\_ISO8601:log\_timestamp} %{LOGLEVEL:log\_level} \[%{DATA:service}\] - %{GREEDYDATA:message}"

]

}

}

}

Sys logs

Mar 14 10:15:43 server1 sshd[12345]: Accepted password for user1 from 192.168.1.15 port 53421 ssh2

Mar 14 10:16:01 server1 CRON[12346]: (root) CMD (/usr/lib/sa/sa1 1 1)

Mar 14 10:17:12 server1 kernel: [123456.789123] eth0: link up

%{SYSLOGTIMESTAMP:syslog\_timestamp} %{HOSTNAME:hostname} %{DATA:process}(?:\[%{POSINT:pid}\])?: %{GREEDYDATA:log\_message}

filebeat.inputs:

- type: log

paths:

- /var/log/test-logs/syslog.log

tags: ["sys"]

- type: log

paths:

- /var/log/test-logs/apache\_access.log

tags: ["apache"]

input {

beats {

port => 5044

}

}

filter {

# For syslog tag

if "sys" in [tags] {

grok {

match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{HOSTNAME:hostname} %{DATA:process}(?:\[%{POSINT:pid}\])?: %{GREEDYDATA:log\_message}" }

}

mutate {

add\_field => { "log\_type" => "syslog" }

}

}

# For apache log tag

if "apache" in [tags] {

grok {

match => { "message" => "%{IPORHOST:client\_ip} %{USER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] \"%{WORD:method} %{URIPATHPARAM:request} HTTP/%{NUMBER:http\_version}\" %{NUMBER:response\_code} %{NUMBER:bytes}" }

}

mutate {

add\_field => { "log\_type" => "apache\_access" }

}

}

}

output {

if "sys" in [tags] {

elasticsearch {

hosts => ["http://localhost:9200"]

index => "logs-sys-%{+YYYY.MM.dd}"

}

}

if "apache" in [tags] {

elasticsearch {

hosts => ["http://localhost:9200"]

index => "logs-apache-%{+YYYY.MM.dd}"

}

}

# Optional stdout for debugging

stdout { codec => rubydebug }

}