**1. Apache Access Logs**

**Sample Logs**

127.0.0.1 - frank [10/Oct/2024:13:55:36 -0700] "GET /apache\_pb.gif HTTP/1.0" 200 2326

192.168.1.1 - john [11/Oct/2024:14:00:21 -0700] "POST /login HTTP/1.1" 401 1420

**Logstash Filter**

ruby

CopyEdit

filter {

grok {

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

}

date {

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

}

}

**✅ 2. Nginx Access Logs**

**Sample Logs**

swift

CopyEdit

192.168.1.10 - - [21/Mar/2024:10:45:32 +0000] "GET /index.html HTTP/1.1" 200 612 "-" "Mozilla/5.0"

**Logstash Filter**

ruby

CopyEdit

filter {

grok {

match => { "message" => "%{IP:client\_ip} - - \[%{HTTPDATE:timestamp}\] \"%{WORD:method} %{URIPATHPARAM:request} HTTP/%{NUMBER:http\_version}\" %{NUMBER:response\_code} %{NUMBER:bytes} \"-\" \"%{DATA:user\_agent}\"" }

}

date {

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

}

useragent {

source => "user\_agent"

target => "user\_agent\_parsed"

}

}

**✅ 3. Linux Syslogs**

**Sample Logs**

nginx

CopyEdit

Mar 21 10:15:42 ubuntu sshd[1234]: Accepted password for user1 from 192.168.1.5 port 54321 ssh2

**Logstash Filter**

filter {

grok {

match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{HOSTNAME:hostname} %{DATA:program}\[%{NUMBER:pid}\]: %{GREEDYDATA:log\_message}" }

}

date {

match => [ "syslog\_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]

}

}

**✅ 4. Windows Event Logs (From Filebeat or Winlogbeat)**

**Sample Logs (JSON format)**

json

CopyEdit

{

"event\_data": {

"TargetUserName": "Administrator",

"LogonType": "10",

"IpAddress": "192.168.1.100"

},

"event\_id": 4624,

"log\_name": "Security",

"record\_number": "123456"

}

**Logstash Filter**

filter {

if [event\_id] == 4624 {

mutate {

add\_field => { "event\_description" => "Successful Logon" }

}

}

}

**✅ 5. IIS Logs**

**Sample Logs**

pgsql

CopyEdit

2024-03-21 14:30:00 W3SVC1 192.168.1.1 GET /index.html - 80 - 192.168.1.100 Mozilla/5.0 200 0 0 15

**Logstash Filter**

ruby

CopyEdit

filter {

grok {

match => { "message" => "%{TIMESTAMP\_ISO8601:log\_timestamp} %{DATA:sitename} %{IP:server\_ip} %{WORD:method} %{URIPATH:uri} %{NOTSPACE:query} %{NUMBER:port} %{NOTSPACE:username} %{IP:client\_ip} %{NOTSPACE:user\_agent} %{NUMBER:response\_code} %{NUMBER:sub\_status} %{NUMBER:win32\_status} %{NUMBER:time\_taken}" }

}

date {

match => [ "log\_timestamp", "YYYY-MM-dd HH:mm:ss" ]

}

}

**✅ 6. JSON Logs**

**Sample Logs**

{"timestamp":"2024-03-21T10:15:30Z","level":"ERROR","service":"payment","message":"Payment failed","user\_id":1234}

**Logstash Filter**

ruby

CopyEdit

filter {

json {

source => "message"

}

date {

match => [ "timestamp", "ISO8601" ]

}

}

**✅ 7. Multiline Java Stack Trace Logs**

**Sample Logs**

Exception in thread "main" java.lang.NullPointerException

at com.example.MyClass.main(MyClass.java:10)

**Logstash Filter**

ruby

CopyEdit

filter {

multiline {

pattern => "^Exception|^\s+at"

what => "previous"

}

grok {

match => { "message" => "%{GREEDYDATA:stack\_trace}" }

}

}

**✅ Additional Useful Filters**

**Mutate (rename, convert, remove)**

ruby

CopyEdit

filter {

mutate {

rename => { "old\_field" => "new\_field" }

convert => { "bytes" => "integer" }

remove\_field => [ "unnecessary\_field" ]

}

}

**GeoIP (for IP address geolocation)**

ruby

CopyEdit

filter {

geoip {

source => "client\_ip"

target => "geoip"

}

}