input {

http {

port => "9642"

type => "watcher"

user => "elastic"

password => "changeme"

#codec => "json"

}

}

filter {

if [type] == "watcher" {

mutate {

add\_field => { "test" => "" }

#add\_field => { "ProcessName" => "" }

#add\_field => { "AccountDomain" => "" }

#add\_field => { "EventLog" => "" }

#add\_field => { "CreatorProcess" => "" }

##add\_field => { "type" => "" }

#add\_field => { "SIDType" => "" }

#add\_field => { "Checksum" => "" }

##add\_field => { "@version" => "" }

##add\_field => { "host" => "" }

#add\_field => { "SecurityID" => "" }

#add\_field => { "ProcessID" => "" }

#add\_field => { "ProcessCommandLine" => "" }

##add\_field => { "timestamp" => "" }

#add\_field => { "Criticality" => "" }

#add\_field => { "severity" => "" }

#add\_field => { "TokenElevationType" => "" }

#add\_field => { "count" => "" }

#add\_field => { "SourceName" => "" }

##add\_field => { "priority" => "" }

#add\_field => { "logsource" => "" }

#add\_field => { "SubmitTime" => "" }

##add\_field => { "tags" => "" }

##add\_field => { "@timestamp" => "" }

#add\_field => { "Username" => "" }

#add\_field => { "ComputerName" => "" }

#add\_field => { "EventID" => "" }

#add\_field => { "CategoryString" => "" }

#add\_field => { "EventLogSource" => "" }

#add\_field => { "facility" => "" }

#add\_field => { "LogonID" => "" }

#add\_field => { "severity\_label" => "" }

#add\_field => { "facility\_label" => "" }

#add\_field => { "AccountName" => "" }

}

#split {

#field => "message"

#}

ruby {

init => "require 'json'"

code => "

message = event.get('message').to\_s

#message.gsub!(/[^0-9A-Za-z]/, ' ')

event.set('message', message)

#terms = Array.new

event\_fields = ['ProcessName=','AccountDomain=','EventLog=','CreatorProcess=','CreatorProcessID=','EventLogType=','type=','SIDType=','Checksum=','@version=','host=','SecurityID=','ProcessID=','ProcessCommandLine=','timestamp=','Criticality=','severity=','TokenElevationType=','count=','SourceName=','priority=','logsource=','SubmitTime=','tags=','@timestamp=','Username=','ComputerName=','EventID=','CategoryString=','EventLogSource=','facility=','LogonID=','severity\_label=','facility\_label=','AccountName=']

start\_ary = Array.new

end\_ary = Array.new

start\_ary = [ 'message=', '@timestamp=', '@version=' ]

end\_ary = [ 'priority=', '@version=', 'AccountDomain=' ]

split\_str = message.split(' ')

new\_str = ''

bad\_str = ''

inside\_message = false

#This parses out the message body setting payload from 2,936 words to 650 words

split\_str.each do |input|

if start\_ary.any?{|w| input.include?(w) }

inside\_message = true

elsif end\_ary.any?{|w| input.include?(w) }

inside\_message = false

end

if !inside\_message

new\_str.concat(input + ' ')

elsif inside\_message

bad\_str.concat(input + ' ')

end

end

event.set('message', new\_str)

#Create Array of WinEvent Fields

# terms = ['EventID:', 'ProcessName:']

#loop until term is found, add value until next term is found

#set field value

field\_value = ''

current\_term = ''

#next\_term = ''

mod\_val = ''

test = ''

get\_val = ''

counter = 1

new\_str.gsub!('=', '= ')

new\_str.gsub!('{', '')

split\_fields = new\_str.split(/[\s,]/)

#current\_term = split\_fields[0]

#next\_term = split\_fields[1]

split\_fields.each\_with\_index do |value, i|

#test.concat(value + ' ')

if event\_fields.include? value

#test.concat(value + ' ')

if !field\_value.empty?

#mod\_val = event\_fields.select{ |s| s.include?(value) }.to\_s

#next\_term.concat(mod\_val + ' ')

if !current\_term.empty?

mod\_val = current\_term.sub('=', ' ')

if !mod\_val.blank?

counter += 1

new\_count = (counter / 30) + 1

get\_val = event.get(mod\_val.to\_s + '')

event.set(mod\_val.to\_s + '', '' + get\_val.to\_s + ' ' + field\_value.to\_s )

end

end

#Reset values

current\_term = value

field\_value = ''

end

else

field\_value.concat(value.to\_s + ' ')

end

end

#event.set('test', mod\_val)

"

}

#mutate {

# gsub => ["message", "\n", ""]

#}

}

}

output {

if [type] == "watcher" {

elasticsearch {

hosts => [ "127.0.0.1:9200" ]

index => "user-activities-%{+YYYY.MM.dd}"

user => "elastic"

password => "changeme"

}

}

}