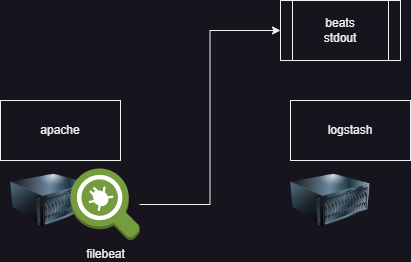
FEBRUARY 16, 2024

DevOps Classroom notes 16/Feb/2024

**Lets build a logstash pipeline**

* Overview  
  
* lets create a vm and install logstash in it
* create one more vm and install apache2 in it and also file beat.
* Now lets create a logstash pipleline
  + input: beats
  + output: stdout
* create a file called as basic.conf in /etc/logstash/conf.d and then lets start the logstash manually

input

{

beats

{

port => 5044

}

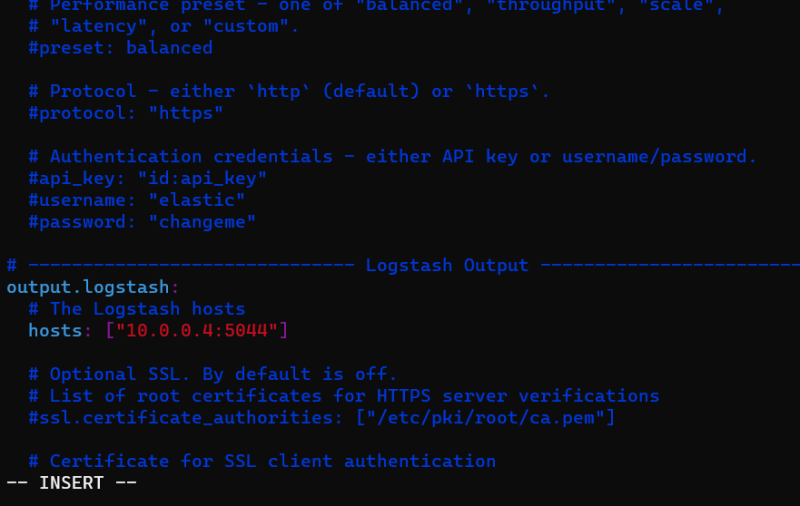
}

output

{

stdout {}

}

* Now change the filebeat.yml to forward logs to logstash on port 5044 on node2  
  
* Lets add a filter grok to extract some field

input

{

beats

{

port => 5044

}

}

filter

{

grok

{

match => { "message" => "%{IP:clientip}%{GREEDYDATA:trimmessage}"}

}

}

output

{

stdout {}

}

* If we have to forward to elastic cloud

input

{

beats

{

port => 5044

}

}

filter

{

grok

{

match => { "message" => "%{IP:clientip}%{GREEDYDATA:trimmessage}"}

}

}

output

{

elasticsearch

{

cloud\_id => ""

cloud\_auth => ""

index => "%{[agent][type]}-%{+YYYY.MM.dd}"

}

}

**Share this:**