Olá pessoal hoje quero trazer um step to step de como configurar um logstash (proxy do Elastic), para se comunicar com a nuvem do Elastic Cloud.

Então lests Go BRO!

O que você vai precisar:

Steps para instalação do Logstash 7.8 no CentOS 8

Toda a configuração aqui tratada é voltada para CentOS 8

Primeiramente instalar o Java

> O CentOS 8 também suporta uma versão decapitada do OpenJDK que fornece um tempo de execução Java mínimo necessário para a execução de aplicativos sem uma interface gráfica do usuário (sem suporte a teclado, mouse e sistemas de exibição). Esta versão é mais adequada para aplicativos de servidor, pois possui menos dependências e usa menos recursos do sistema.

Para instalar use o comando abaixo:

sudo dnf install java-11-openjdk-headless

Instalando o logstash:

Primeiro passo, fazer o download da licença do Logstash

sudo rpm –import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Adicionar o repositório oficial do elastic:

- Ir para a o diretório de repositório e criar um arquivo de repo (aqui deixei nomeado como elasticsearch).

cd /etc/yum.repos.d/
vim elasticsearch.repo

- Inserir o seguinte conteúdo

```
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Após salve e saia

Em seguida verifique o repositório disponível no sistema.

dnf repolist

NOTA: É aconselhável adicionar o repo, pois o elastic possui algumas dependências próprias.

Em seguida fazer o Download do RPM no site oficial do Elastic
NOTA: Aqui é tratada a versão 7.8

Link: https://www.elastic.co/pt/downloads/logstash

No exemplo acima fiz o download por wget fique à vontade para enviar o arquivo com outras ferramentas.

Agora efetue a instalação com o comando:

rpm -ivh logstash-7.8.0.rpm

Agora o Logstash já está instalado.

Porém é necessário configurar mais alguns arquivos antes de iniciar o serviço.

Vá para o diretório:

cd /etc/logstash/conf.d/

Agora crie um arquivo logstash.conf

vim logstash.conf

Dentro dele coloque o seguinte arquivo

NOTA: Indentação é boa prática

```
input {
  beats {
    port => 5043
    type => beats
  }
  tcp {
    port => 5046
    codec => "json"
    type => tcp
  }
}

filter {
    if "beats_input_codec_plain_applied" in [tags] {
        mutate {
          remove_tag => ["beats_input_codec_plain_applied"]
          add_field => [ "received_at", "%{@timestamp}" ]
          add_field => [ "received_from", "%{host}" ]
        }
    } else {
        mutate {
          lowercase => ["appName"]
          add_field => [ "received_at", "%{@timestamp}" ]
          add_field => [ "received_from", "%{host}" ]
       }
    }
}

output {
   if [type] == "beats" {
     elasticsearch {
            user => elastic
            password => "password"
            index => "%{tags}-%{+yyyy.MM.dd}"
            hosts => ["https://assinaturanacloud.us-east-1.aws.found.io:9243"]
     }
     stdout { codec => rubydebug }
   }
   if[type] == "tcp" {
        elasticsearch {
             user => elastic
             password => "password"
             index => "%{appName}-%{+yyyy.MM.dd}"
             hosts => ["https://assinaturanacloud.us-east-1.aws.found.io:9243"]
        }
   }

}
```

Esse arquivo adiciona dois campos no filtro:

Timestamp e Host

E já trabalha duas entradas uma por beats e outra por tcp

E no output ele trata 4 saídas distintas separando para log, tcp, beats e uma saída que trata tipos não mapeados no “else”

Mais um ponto importante é necessário colocar o endpoint do elastic e a senha do mesmo que é entregue ao criar o deployment na SaaS da Elastic.

Que apresento a seguir:

Faça o login na sua conta:

NOTA: Aqui irei seguir baseado no entendimento que o administrador já criou o deployment, posteriormente farei uma doc ensinando está parte.

No console acesse o Deployment que está em uso:

Nesta parte clique em copy endpoint e em seguida guarde essa URL.

Ao lado você terá o Cloud ID Copie o mesmo também e guarde.

O usuário e senha do elastic e gerado ao criar o Deployment, sempre verifique com o administrador ou responsável que gerou esse acesso.

Caso seja feito o reset de senha a mesma ira impactar todas as soluções configuradas com estas credenciais.

Voltando ao arquivo de configuração adicione o endpoint do Elastic em hosts

Adicione o password obtido no console do Elastic onde está marcado como password.

Com o arquivo configurado agora precisamos inserir as credenciais da cloud.

Vá para o diretório:

cd /etc/logstash

E vamos editar o arquivo logstash.yml

Dentro do arquivo localize a sessão Cloud Settings aqui vamos precisar alterar

alguns dados.

Vamos precisar adicionar o Cloud ID que você copiou na console.

E o usuário e senha do deployment neste formato:

elastic:minhasenhalegal

O usuário e separado da senha através “:”

Feito o Ajuste salve e saia

Agora vamos testar a comunicação:

Vá para o diretório:

cd /usr/share/logstash

E execute o seguinte comando:

bin/logstash –modules netflow -M “netflow.var.input.udp.port=3555” —cloud.id AQUI_VAI_O_SEU_CLOID_ID –cloud.auth USUARIO:SENHA_ELASTIC

O retorno será algo assim se não houver problemas de comunicação:

NOTA: atente-se para a última linha:

Uma dica a partir deste diretório, você pode verificar se o seu arquivo de configuração do logstash.conf está correto com o comando:

bin/logstash -f logstash.conf

A saída já mostra de houve comunicação e se está ok.

Após todos os steps vamos iniciar o Logstash e colocar para iniciar com a máquina.

Comandos:

systemctl start logstash

systemctl enable logstash

Agora é só confirmar com o:

systemctl status logstash

Finalizado, Logstash configurado com o Elastic Cloud e pronto para receber os logs.