Instalação agente logstash

1 - Adicionar a Key Public do repositorio Elastic.co ao servidor que será realizada a instalação:

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

2 - Navegue até o diretório de repositórios do CentOS:

# cd /etc/yum.repos.d/

3 - Crie o arquivo logstash.repo:

# sudo touch logstash repo

4 - Edite o arquivo recém criado adicionando as seguintes informações:

# sudo vim logstash.repo

[logstash-8.x]

name=Elastic repository for 8.x packages

baseurl=https://artifacts.elastic.co/packages/8.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

5 - Realize a instalação do Agente:

# sudo yum install logstash

6 - Configurando o agente:

6.1 - importe os arquivos para os seus respectivos diretórios:

Arquivos config

# mv /config/losgatsh.yml /etc/logstash/

# mv /config/pipeline.yml /etc/logstash/

Arquivos pipeline

# mv /pipeline/httpd\_logstash.conf /etc/logstash/conf.d/

# mv /pipeline/wildfly\_logstash.conf /etc/logstash/conf.d/

OBS: O nome do indice deve ser alterado dentro do arquivo de pipeline de acordo com o ambiente na ultima linha de cada “.conf” para melhor identificação dos documentos.



6.2 - ative o serviço logstash:

# sudo systemctl enable logstash.sevice && systemctl start logstash