ELK Elasticstack – Dia 1

1. Instruções

2. Introdução

- Instalar
- Configurar
- Indexar
- Manter

3. Material para Download

- Scripts
- Slides em PDF
- Dados

4. Apresentação

Iremos estudar a Stack ELK

5. O que Vamos Estudar?

ELK stack é um acrônimo que descreve uma pilha de três projetos de código aberto: **Elasticsearch** , **Logstash** e **Kibana** . A pilha fornece visibilidade dos logs do(s) seu(s) sistema(s) e aplicativos, analisa-os e cria belas visualizações em painéis personalizados para monitoramento, análise e solução de problemas. Vamos dar uma olhada em cada um dos elementos:

Elasticsearch:

{HYPERLINK "https://www.elastic.co/elasticsearch"**}** é um mecanismo de pesquisa e análise de alto desempenho RESTful distribuído, construído no Apache Lucene. É uma escolha ideal para análise de logs, dado seu suporte para documentos JSON sem esquema e suporte para uma miríade de idiomas.

Logstash:

{HYPERLINK "https://www.elastic.co/logstash"**}**é um pipeline de processamento de dados leve, do lado do servidor, que coleta dados de várias fontes, os transforma e os envia para o destino desejado, por exemplo, Elasticsearch.

Kibana:

Kibana é uma interface de usuário de web de dados de código aberto e ferramenta de visualização de dados para visualizar logs coletados e processados pelo Logstash e Elasticsearch. Ele oferece recursos poderosos e fáceis de usar, como histogramas, gráficos de linha, gráficos de pizza, mapas de calor e suporte geoespacial integrado.

6. O Ambiente para o Curso

7. Instalando Virtual Box

https://www.virtualbox.org/wiki/Downloads

8. Download Ubuntu Server

https://ubuntu.com/download/server

9. Instalando Ubuntu Server

{HYPERLINK "https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox" \t "_blank"}

10. Instalando Ubuntu Server Parte II

{HYPERLINK "https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox" \t "_blank"}

11. Instalando Elasticsearch

ELK stack é um acrônimo que descreve uma pilha de três projetos de código aberto: Elasticsearch , Logstash e Kibana . A pilha fornece visibilidade dos logs do(s) seu(s) sistema(s) e aplicativos, analisa-os e cria belas visualizações em painéis personalizados para monitoramento, análise e solução de problemas. Vamos dar uma olhada em cada um dos elementos:

Elasticsearch:

Elasticsearch é um mecanismo de pesquisa e análise de alto desempenho RESTful distribuído, construído no Apache Lucene. É uma escolha ideal para análise de logs, dado seu suporte para documentos JSON sem esquema e suporte para uma miríade de idiomas.

Logstash:

Logstash é um pipeline de processamento de dados leve, do lado do servidor, que coleta dados de várias fontes, os transforma e os envia para o destino desejado, por exemplo, Elasticsearch.

Kibana:

Kibana é uma interface de usuário de web de dados de código aberto e ferramenta de visualização de dados para visualizar logs coletados e processados pelo Logstash e Elasticsearch. Ele oferece recursos poderosos e fáceis de usar, como histogramas, gráficos de linha, gráficos de pizza, mapas de calor e suporte geoespacial integrado.

Como instalar o Elastic (ELK) Stack no Ubuntu 24.04
Sem mais delongas, vamos nos aprofundar nas etapas de instalação do ELK.

12. Instalação do Elasticsearch

1) Instale o Java

Como o Elasticsearch é desenvolvido em Java, você deve instalar o Java como pré-requisito. Antes disso, garanta que seu sistema esteja atualizado executando os comandos:

```
$ sudo apt update
$ sudo apt upgrade -y
```

Instalaremos o OpenJDK 17, a versão LTS estável mais recente que fornece Java. Para isso, instale-o a partir dos repositórios padrão do Ubuntu usando o gerenciador de pacotes APT.

```
$ sudo apt install openjdk-17-jdk -y
```

Para confirmar se o Java está instalado, execute o comando:

```
$ java -version
```

2) Adicionar repositório Elastic Stack

Por padrão, todos os três componentes da pilha ELK não estão disponíveis nos repositórios apt do Ubuntu. Portanto, você precisa adicionar manualmente a lista de fontes de pacotes do Elastic. Para fazer isso, primeiro adicione a Chave GPG.

```
$ wget https://artifacts.elastic.co/GPG-KEY-elasticsearch -O /etc/apt/keyrings/GPG-KEY-elasticsearch.key
```

Em seguida, adicione o Repositório Elasticsearch:

```
$ echo "deb [signed-by=/etc/apt/keyrings/GPG-KEY-elasticsearch.key] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

Em seguida, atualize as listas de pacotes locais para notificar o sistema sobre o repositório recém-adicionado.

```
$ sudo apt update
```

Com o cache APT local atualizado, agora você pode instalar o Elasticsearch.

3) Instale o Elasticsearch

Para instalar o Elasticsearch, execute o comando:

```
$ sudo apt install elasticsearch -y
```

Quando a instalação estiver concluída, as ‘security autoconfiguration information‘ serão impressas na tela.

Quando a instalação estiver concluída, inicie o serviço Elasticsearch executando os comandos abaixo.

```
$ sudo systemctl daemon-reload
$ sudo systemctl start elasticsearch
```

Considere também habilitar o serviço Elasticsearch para iniciar automaticamente após a instalação.

```
$ sudo systemctl enable elasticsearch
```

Para confirmar se o Elasticsearch está em execução, execute o comando:

```
$ sudo systemctl status elasticsearch
```

4) Configurar Elasticsearch

Antes de prosseguir, você precisa fazer algumas modificações no Elasticsearch. Portanto, acesse o arquivo de configuração do Elasticsearch.

```
$ sudo nano /etc/elasticsearch/elasticsearch.yml
```

Para começar, certifique-se de dar um nome descritivo ao seu cluster, descomentando a diretiva cluster.name e fornecendo seu nome preferido.

Aqui, nomeamos nosso cluster de sample-cluster.

```
cluster.name: sample-cluster
```

Em seguida, forneça um nome descritivo para o nó descomentando a diretiva node.name.

```
node.name: elasticsearch-node
```

Por padrão, o Elasticsearch só é acessível no localhost. Para torná-lo acessível ao mundo externo, descomente e atualize o atributo `network.host` handset-o para 0.0.0.0.

```
network.host: 0.0.0.0
```

Em seguida, localize a diretiva xpack.security.enabled: e defina-a como falsa.

```
xpack.security.enabled: false
```

Salve as alterações e saia do arquivo de configuração. Para aplicar as alterações, reinicie o Elasticsearch

```
$ sudo systemctl restart elasticsearch
```

Para verificar se o serviço Elasticsearch está em execução, envie uma solicitação HTTP usando o utilitário Curl, conforme mostrado.

```
$ curl -X GET "localhost:9200"
```

Você deve receber uma resposta com algumas informações básicas sobre seu nó local:

Além disso, você pode fazer isso a partir de um navegador da web.

```
http://ip_do_servidor:9200
```

5) Instale o Kibana

O próximo componente a ser instalado é o Kibana. Esta é uma poderosa ferramenta de exploração e visualização de dados baseada na web para visualizar logs e dados de séries temporais. Ela oferece painéis poderosos e ricos em recursos e uma variedade de gráficos, como gráficos de barras, gráficos de pizza, histogramas, mapas de calor, etc.

Para instalar o Kibana, execute o comando:

```
$ sudo apt install kibana -y
```

Após a instalação, inicie e ative o Kibana para iniciar automaticamente.

```
$ sudo systemctl start kibana
```

```
$ sudo systemctl enable kibana
```

Você pode verificar o status do Kibana executando:

```
$ sudo systemctl status kibana
```

O Kibana escuta na porta TCP 5601 por padrão. Você pode confirmar isso executando o comando:

```
$ sudo ss -pnltu | grep 5601
```

6) Configurar o Kibana

Alguns ajustes adicionais são necessários no Kibana para uma experiência tranquila e para permitir que ele funcione com outros componentes.

Então, acesse o arquivo de configuração do Kibana.

```
$ sudo nano /etc/kibana/kibana.yml
```

Descomente a linha abaixo.

```
server.port: 5601
```

Para permitir conexões de usuários remotos, defina a diretiva server.host como 0.0.0.0.

```
server.host: 0.0.0.0
```

Além disso, descomente a seguinte linha

```
elasticsearch.hosts: ["http://localhost:9200"]
```

Salve as alterações e saia. Para aplicar as alterações feitas, reinicie o Kibana.

```
$ sudo systemctl restart kibana
```

Para acessar o Kibana pelo seu navegador, visite o seguinte URL.

```
http://ip-do-servidor:5601
```

Além disso, você pode ter uma visão geral do status e dos serviços disponíveis visitando o seguinte URL.

http://server-ip:5601/status

7) Instalar Logstash

O próximo componente a ser instalado será o Logstash. Este pipeline processa e envia dados para o Elasticsearch para indexação e armazenamento. Para instalar o Logstash, execute o comando:

```
$ sudo apt install logstash -y
```

Após a instalação, inicie e habilite o Logstash executando os seguintes comandos

```
$ sudo systemctl start logstash
$ sudo systemctl enable logstash
```

Para verificar o status do log stash, execute o comando:

```
$ sudo systemctl status logstash
```

8) Configurar Logstash

Como mencionado anteriormente, o Logstash é um pipeline que analisa e processa dados e os envia para o destino desejado, neste caso, o Elasticsearch.

Um pipeline consiste em dois elementos obrigatórios: entrada e saída. O elemento filter é opcional. O plugin input pega ou ingere dados da fonte. Os filtros são plugins intermediários que processam dados enquanto o plugin output envia e grava dados em um destino.

Seguindo em frente, crie um arquivo de configuração chamado 02-beats-input.conf. É aqui que você vai configurar sua entrada Filebeat:

```
$ sudo nano /etc/logstash/conf.d/02-beats-input.conf
```

Adicione as seguintes linhas de código:

```
input {
  beats {
    port => 5044
  }
}
```

Em seguida, crie um arquivo de configuração chamado 30-elasticsearch-output.conf:

```
$ sudo nano /etc/logstash/conf.d/30-elasticsearch-output.conf
```

A saída configura o Logstash para armazenar os dados do Beats no Elasticsearch, rodando em localhost:9200. Usamos o Beats como índice. Neste tutorial, os beats serão suportados pelo filebeat.

```
output {
  if [@metadata][pipeline] {
     elasticsearch {
     hosts => ["localhost:9200"]
     manage_template => false
     index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
     pipeline => "%{[@metadata][pipeline]}"
     }
  } else {
     elasticsearch {
     hosts => ["localhost:9200"]
     manage_template => false
     index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
```

```
    }
  }
}
```
Salvar e sair. Para testar a configuração do Logstash, execute o comando:

```
$ sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t
```

A saída compreende um bloco de linhas de código com a string – Resultado da validação de configuração: OK. Saindo do Logstash – exibido no final. Se você não vir isso na sua saída, certifique-se de revisar sua configuração do Logstash para erros

Para efetuar as alterações, certifique-se de reiniciar o logstash

```
$ sudo systemctl restart logstash
```

9) Instalar e configurar o Filebeat

O último componente a ser instalado é o Filebeat. Este é um dos carregadores leves que encaminha dados de log centralizados para o Elasticsearch ou Logstash, dependendo de como ele está configurado.

Para instalar o Filebeat, execute o comando:

```
$ sudo apt install filebeat -y
```
Em seguida, configuraremos o Filebeat para enviar dados ao Logstash. Então, acesse o arquivo de configuração do Filebeat:

```
$ sudo nano /etc/filebeat/filebeat.yml
```
Configuraremos o Filebeat para enviar dados diretamente para o Logstash para processamento em vez do Elasticsearch. Portanto, desabilitaremos a saída do Elasticsearch. Para fazer isso, localize a seção ` output.elasticsearch ` e comente as seguintes linhas:

```
...
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: ["localhost:9200"]
…
```
Em seguida, configuraremos o Filebeat para se conectar ao Logstash no servidor Elastic Stack na porta 5044. Para fazer isso, descomente as linhas ` output.logstash: ` e ` hosts: [“localhost:5044”] `.

```
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```
Uma vez feito isso, salve as alterações e saia.

Os módulos Filebeat estendem a funcionalidade do Filbeat. Aqui, habilitaremos o módulo do sistema que coleta e analisa logs gerados pelo serviço de log do sistema.

Para obter uma lista de todos os módulos disponíveis, execute o comando:

```
$ sudo filebeat modules list
```

Para habilitar o módulo do sistema, execute o comando:

```
$ sudo filebeat modules enable system
```

Em seguida, você precisa configurar os pipelines de ingestão do Filebeat. Os pipelines analisam os dados de log antes de passá-los pelo Logstash para o Elasticsearch. Execute o comando a seguir para carregar o pipeline de ingestão para o módulo do sistema.

```
$ sudo filebeat setup --pipelines --modules system
```

Em seguida, você precisa carregar o modelo de índice no Elasticsearch. Um índice é simplesmente um conjunto de documentos com características semelhantes. Para carregar o modelo, execute o comando:

$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

Por padrão, o Filebeat fornece dashboards de amostra do Kibana para visualizar dados do Filebeat no Kibana. Portanto, antes de usar os dashboards, é imperativo criar o padrão de índice primeiro e carregar os dashboards no Kibana.

Para fazer isso, execute o comando:

$ sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601

A partir daqui, inicie e ative o Filebeat.

$ sudo systemctl start filebeat
$ sudo systemctl enable filebeat
Não deixe de verificar seu status

$ sudo systemctl status filebeat

Agora, altere as configurações usando o vi:

sudo vi /etc/elasticsearch/elasticsearch.yml
Remova o comentário (#) da linha node.nome, para isso coloque o vi em modo de inserção teclando i

Altere network.host para 0.0.0.0

Altere discovery.seed.hosts para [“127.0.0.1”]

E cluster.initial_master_nodes para [“node-1”]

Quando terminar, tecle ESC para sair do modo de inserção, então digite :wq para salvar e sair do vi.

Execute os comandos abaixo para iniciar o Elasticsearch e para configurar a inicialização automática.

sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service

O serviço pode levar alguns minutos até estar pronto.

13. Testando Elasticsearch

1. Baixar o template:

wget http://media.sundog-soft.com/es8/shakes-mapping.json

2. Criar o index:

curl -H 'Content-Type: application/json' -XPUT 127.0.0.1:9200/shakespeare --data-binary @shakes-mapping.json
wget http://media.sundog-soft.com/es8/shakespeare_8.0.json

3. Enviar os dados para o index Shakespeare criado no elk

```
curl -H 'Content-Type: application/json' -XPOST
'127.0.0.1:9200/shakespeare/_bulk?pretty' --data-binary
@shakespeare_8.0.json
```

4. Consultar os dados no elk

```
curl -H 'Content-Type: application/json' -XGET
'127.0.0.1:9200/shakespeare/_search?pretty' -d '
{
"query" : {
"match_phrase" : {
"text_entry" : "to be or not to be"
}
}
}
'
```