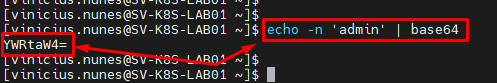
**CRIANDO SECRET VIA MANIFEST FILE**

PASSO 1 - Execute o comando abaixo, para que possamos gerar um valor base64 para o usuário que utilizaremos no arquivo manifesto da secret em questão, e então, copie e guarde o resultado da saída stdout, pois o valor em questão será utilizado nos próximos passos.

COMANDO: **echo -n 'DIGITE\_O\_NOME\_DO\_USUÁRIO\_QUE\_SERÁ\_UTILIZADO' | base64**

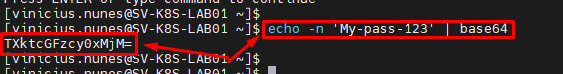
EXEMPLO:



PASSO 2 - Execute o comando abaixo, para que possamos gerar um valor base64 para a senha do usuário que utilizaremos no arquivo manifesto da secret em questão, e então, copie e guarde o resultado da saída stdout, pois o valor em questão será utilizado nos próximos passos.

COMANDO: **echo -n 'DIGITE\_A\_SENHA\_QUE\_DESEJA\_UTILIZAR\_NO\_USUÁRIO\_QUE\_SERÁ\_UTILIZADO' | base64**

EXEMPLO:



PASSO 3 - Execute o comando abaixo, para que criar o arquivo manifesto programado em YAML\YML.

COMANDO: **sudo vim /DIGITE\_O\_DIRETORIO\_COMPLETO/DIGITE\_O\_NOME\_DO\_ARQUIVO.yml**

EXEMPLO:

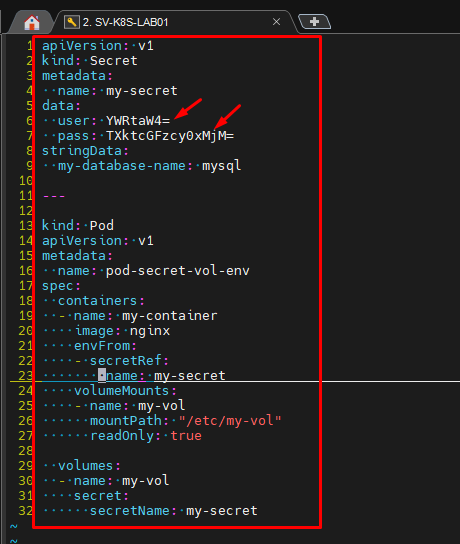


PASSO 4 - Insira o conteúdo desejado dentro do arquivo em questão, se atentando a "IDENTAÇÃO" do conteúdo a ser inserido.

EXEMPLO DE CONTEÚDO:

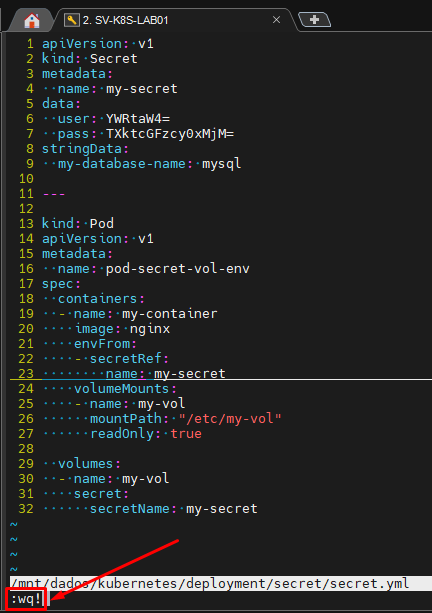
**OBSERVAÇÃO IMPORTANTE 1:** Na chave "user", insira o conteúdo copiado da saída do comando executado no PASSO 1.

**OBSERVAÇÃO IMPORTANTE 2:** Na chave "pass", insira o conteúdo copiado da saída do comando executado no PASSO 2.



PASSO 5 - Salve o arquivo em questão, através da combinação de teclas SHIFT + : (DOIS PONTOS DO TECLADO) + wq + ! (Sinal de exclamação).

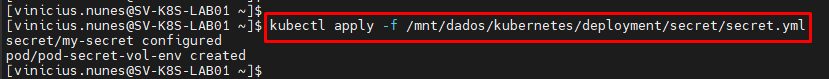
EXEMPLO:



PASSO 6 - Execute o comando abaixo, para que possamos executar o arquivo manifesto criado anteriormente.

COMANDO: **kubectl apply -f /DIGITE\_O\_CAMINHO\_ABSOLUTO\_DO\_DORETÓRIO/DIGITE\_O\_NOME\_DO\_ARQUIVO.yml**

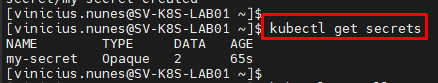
EXEMPLO:



PASSO 7 - Execute o comando abaixo, para que possamos visualizar o secret criado anteriormente em execução.

COMANDO: **kubectl get secrets**

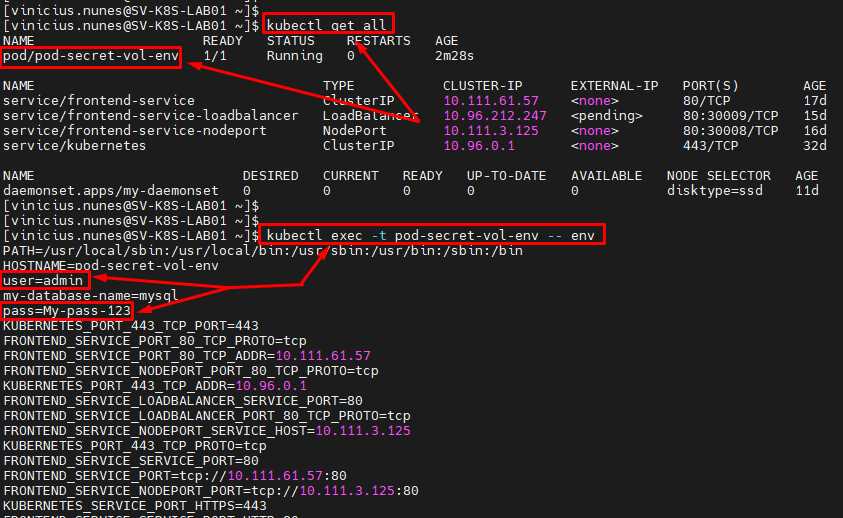
EXEMPLO:



PASSO 8 - Agora execute o comando abaixo, para que possamos validar se os valores das variáveis que aplicamos a ação de base64 (hash) no usuário e senha, estão sendo reconhecidos com o usuário e senha corretamente dentro do container do POD.

COMANDO: **kubectl exec -t DIGITE\_O\_NOME\_DO\_POD\_QUE\_CRIAMOS\_ANTERIORMENTE -- env**

EXEMPLO:



PASSO 9 - Pronto, agora basta seguir com a utilização do recurso em questão em seu ambiente.