Password security procedure

openssl genrsa -aes256 -out cert.pem -passout pass:changeit 4096

openssl rsa -in cert.pem -out private.pem -passin pass:changeit

openssl rsa -in cert.pem -passin pass:changeit -pubout > public.pem

create cred.txt file and include password as asdf1234

openssl pkeyutl -encrypt -inkey public.pem -pubin -in cred.txt | openssl base64 -A > encrypt.txt

cat encrypt.txt | openssl base64 -A -d | openssl pkeyutl -decrypt -inkey private.pem > decrypt.txt

flags once encryption is done we place this encryption.txt file config map lo pedtam we set it as a volume in container.

kubectl create configmap tomcat --from-file=encrypt.txt

kubectl exec -i -t tomcat-79b8ddb9dc-shsvg --container tomcat -- /bin/bash

kubectl exec -i -t tomcat-79b8ddb9dc-shsvg --container tomcat -- /bin/bash

before app start we retrieve above by using script and we keep it in shell and we expose it in .env file

Catalina.sh

#!/bin/bash

cd /opt/tomcat

cat encrypt.txt | openssl base64 -A -d | openssl pkeyutl -decrypt -inkey private.pem > decrypt.txt

export DBUSER=xxxxx

export DBPASS=$(cat decrypt.txt)

root@ip-172-31-7-14:~# history

1 cd

2 pwd

3 sudo apt-get update && sudo apt-get upgrade

4 sudo apt install build-essential checkinstall zlib1g-dev -y

5 cd /usr/local/src/

6 wget https://www.openssl.org/source/openssl-1.1.1k.tar.gz

7 tar -xf openssl-1.1.1k.tar.gz

8 cd openssl-1.1.1k.tar.gz

9 tar -xf openssl-1.1.1k.tar.gz

10 cd openssl-1.1.1k.tar.gz

11 ./config --prefix=/usr/local/ssl --openssldir=/usr/local/ssl shared zlib

12 cd ../..

13 cd ..

14 openssl

15 openssl version

16 cd

17 clear

18 openssl -aes256 -out private.pem -passout pass:changeit 4096

19 openssl genrsa -aes256 -out private.pem -passout pass:changeit 4096

20 ls

21 rm -rf private.pem

22 openssl genrsa -aes256 -out cert.pem -passout pass:changeit 4096

23 openssl rsa -in cert.pem -out private.pem -passin pass:changeit

24 ls

25 openssl rsa -in cert.pem -passin pass:changeit -pubout > public.pem

26 ls

27 vi cred.txt

28 openssl rsautl -encrypt -inkey public.pem -pubin -in cred.txt | openssl base64 -A > encrypt.txt

29 openssl pkeyutl -encrypt -inkey public.pem -pubin -in cred.txt | openssl base64 -A > encrypt.txt

30 ls

31 cat encrypt.txt

32 clear

33 ls

34 cat encrypt.txt | openssl base64 -A -d | openssl pkeyutl -decrypt -inkey private.pem > decrypt.txt

35 ls

36 cat decrypt.txt

37 history

root@ip-172-31-7-14:~# ^C

root@ip-172-31-7-14:~#