Welcome to ExamTopics

EXAMTOPICS

- Expert Verified, Online, **Free**.

MENU

Google Discussions

Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

Go to Exam

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 42 DISCUSSION

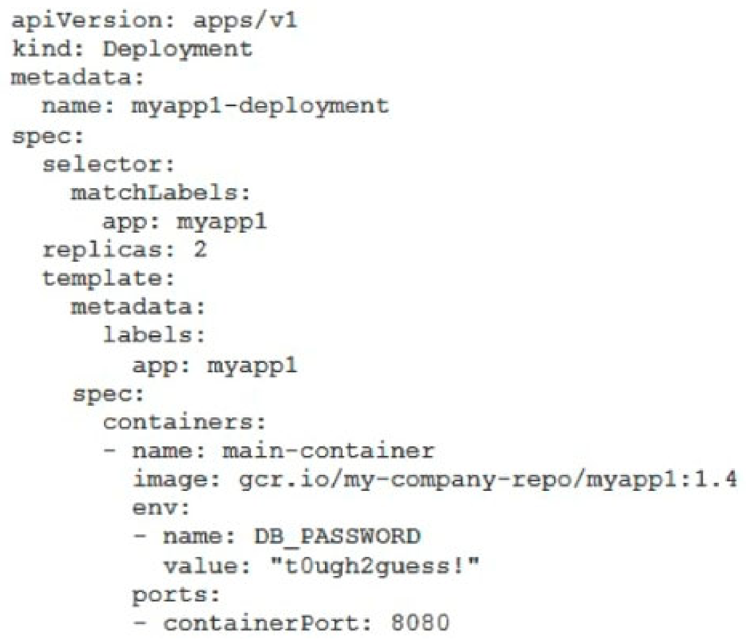
Actual exam question from Google's Associate Cloud Engineer

Question #: 42

Topic #: 1

[All Associate Cloud Engineer Questions]

You've deployed a microservice called myapp1 to a Google Kubernetes Engine cluster using the YAML file specified below:



```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: myapp1-deployment
spec:
  selector:
    matchLabels:
      app: myapp1
  replicas: 2
  template:
    metadata:
      labels:
        app: myapp1
    spec:
      containers:
      - name: main-container
        image: gcr.io/my-company-repo/myapp1:1.4
        env:
        - name: DB_PASSWORD
          value: "t0ugh2guess!"
        ports:
        - containerPort: 8080
```

You need to refactor this configuration so that the database password is not stored in plain text. You want to follow Google-recommended practices. What should you do?

A. Store the database password inside the Docker image of the container, not in the YAML file.

B. Store the database password inside a Secret object. Modify the YAML file to populate the DB_PASSWORD environment variable from the Secret.

C. Store the database password inside a ConfigMap object. Modify the YAML file to populate the DB_PASSWORD environment variable from the ConfigMap.

D. Store the database password in a file inside a Kubernetes persistent volume, and use a persistent volume claim to mount the volume to the container.

Show Suggested Answer

by rramani7 at *June 1, 2020, 3:01 a.m.*

Comments

Type your comment...

Submit

rramani7 **Highly Voted** 4 years, 4 months ago

it is good practice to use Secrets for confidential data (like API keys) and ConfigMaps for non-confidential data (like port numbers). B is correct.

upvoted 72 times

saurabh1805 **Highly Voted** 4 years, 4 months ago

B is correct answer
https://cloud.google.com/kubernetes-engine/docs/concepts/secret

upvoted 39 times

hjyhf 3 years, 2 months ago

"Storing sensitive data in Secrets is more secure than in plaintext ConfigMaps or in Pod specifications"

upvoted 9 times

559b96d **Most Recent** 4 months, 2 weeks ago

How could this possibly be C over B?

"ConfigMap is similar to Secret except that you use a Secret for sensitive information and you use a ConfigMap to store non-sensitive data such as connection strings, public credentials, hostnames, and URLs."

upvoted 2 times

subha.elumalai 5 months ago

Correct Answer: C

upvoted 1 times

Sandy8 9 months, 4 weeks ago

In my opinion also B is correct answer as secret manager will keep secret of all credentials and confidentiality.

upvoted 1 times

Mohit__ 10 months ago

why most answer by examtopics are wrong

upvoted 3 times

gsmasad 11 months, 3 weeks ago

Selected Answer: B

B is correct because storing passwords in secrets is the GKE best practice

upvoted 1 times

bearfromoso 1 year ago

Storing database passwords, or any sensitive credentials, inside a ConfigMap is not recommended from a security standpoint. "B" it is!

upvoted 1 times

Captain1212 1 year, 1 month ago

Selected Answer: B

Selected Answer: B

b is correct as it good pracits to use secrrets for the passwords

upvoted 1 times

bobthebuilder_karkedikhayenge 1 year, 1 month ago

Selected Answer: B

correct answer is B, as secrets are used to store credentials and configmap is used to store the configuration

upvoted 1 times

sthapit 1 year, 2 months ago

B is the right approach

upvoted 1 times

ExamsFR 1 year, 3 months ago

Selected Answer: B

B is correct.

upvoted 1 times

raselsys 1 year, 7 months ago

B is the correct answer as configmap is configurations non confidential.

upvoted 1 times

PB78 1 year, 7 months ago

A common use case for a service is to use ConfigMaps to separate application code from configuration. ConfigMap is similar to Secret except that you use a Secret for sensitive information and you use a ConfigMap to store non-sensitive data such as connection strings, public credentials, hostnames, and URLs.

upvoted 1 times

Buruguduystunstugudunstuy 1 year, 8 months ago

Selected Answer: B

Answer B is the correct choice as it recommends storing the database password inside a Secret object, which is designed to securely store sensitive data like passwords, and then modifying the YAML file to populate the DB_PASSWORD environment variable from the Secret.

Storing sensitive information such as passwords in plain text inside configuration files is not secure and violates Google's security best practices. Instead, secrets should be stored separately and securely. In Kubernetes, secrets are designed to store sensitive information such as passwords, API keys, and tokens. Secrets are encrypted and can be used to pass sensitive data to containers in a safe manner.

To implement this in the given configuration, you can create a secret object and store the database password as a key-value pair. Then, modify the YAML file to populate the DB_PASSWORD environment variable from the secret.

https://kubernetes.io/docs/concepts/configuration/secret/

upvoted 1 times

Di4sa 1 year, 8 months ago

B is the correct answer
A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Such information might otherwise be put in a Pod specification or in a container image. Using a Secret means that you don't need to include confidential data in your application code.

upvoted 1 times

glanshima 1 year, 8 months ago

Selected Answer: B

B not C read here that configmap don't encrypt
https://kubernetes.io/docs/concepts/configuration/configmap/

upvoted 1 times

Load full discussion...

Social Media

Facebook , Twitter

YouTube , Reddit

Pinterest

EXAMTOPICS

We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.