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 263 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 263

Topic #: 1

[All Associate Cloud Engineer Questions]

Your customer wants you to create a secure website with autoscaling based on the compute instance CPU load. You want to enhance performance by storing static content in Cloud Storage. Which resources are needed to distribute the user traffic?

A. An external HTTP(S) load balancer with a managed SSL certificate to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend.

B. An external network load balancer pointing to the backend instances to distribute the load evenly. The web servers will forward the request to the Cloud Storage as needed.

C. An internal HTTP(S) load balancer together with Identity-Aware Proxy to allow only HTTPS traffic.

D. An external HTTP(S) load balancer to distribute the load and a URL map to target the requests for the static content to the Cloud Storage backend. Install the HTTPS certificates on the instance.

Show Suggested Answer

by KelvinToo at *Dec. 31, 2023, 6:28 p.m.*

Comments

Type your comment...

Cynthia2023 `Highly Voted` 9 months, 3 weeks ago

`Selected Answer: A`

Why D is not correct:
Installing HTTPS Certificates on the Instance: While this approach can work, it's generally more efficient and secure to use a managed SSL certificate with the load balancer itself, rather than installing and managing certificates on each individual instance. Managing SSL certificates on the load balancer simplifies certificate management, especially in an autoscaling environment where new instances are frequently created and removed.

upvoted 7 times

yomi95 1 week, 4 days ago

Option A: preferred.
Uses an external HTTP(S) load balancer with a managed SSL certificate. This means that the SSL certificate is managed by Google Cloud, and you don't need to install or renew it on your compute instances. This simplifies the management of your website and ensures that it is always accessible over HTTPS.

Option D:
Uses an external HTTP(S) load balancer but requires you to install the HTTPS certificates on the instance. This means that you are responsible for managing and renewing the certificates, which can be more complex and time-consuming.

upvoted 1 times

kuracpalac 7 months, 3 weeks ago

I'd say because the answer contains "Install the HTTPS certificates on the instance.", which is not a good way to go about things. You;d want the managed SSL cert (ans A) so that you don't have to worry about it. So A makes more sense.

upvoted 3 times

TanTran04 `Most Recent` 7 months ago

`Selected Answer: A`

Choose option A

upvoted 1 times

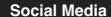**KelvinToo** 9 months, 3 weeks ago

`Selected Answer: A`

ChatGPT says the answer is A.

upvoted 1 times

KelvinToo 9 months, 3 weeks ago

Option A aligns with the requirements of security, autoscaling, and performance optimization by leveraging Cloud Storage for static content while efficiently distributing user traffic.

upvoted 1 times

Social Media

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.