EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 103 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 103
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You are designing a new governance model for your organization's secrets that are stored in Secret Manager. Currently, secrets for Production and Non-
Production applications are stored and accessed using service accounts. Your proposed solution must:

- Provide granular access to secrets
- Give you control over the rotation schedules for the encryption keys that wrap your secrets
- Maintain environment separation
- Provide ease of management

Which approach should you take?

A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

B. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.

C. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings. 3. Use Google-managed encryption keys to encrypt secrets.

D. 1. Use a single Google Cloud project to store both Production and Non-Production secrets. 2. Enforce access control to secrets using project-level Identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

Show Suggested Answer

by mT3 at *May 19, 2022, 3:15 p.m.*

Comments

Type your comment...

Submit

mT3 Highly Voted 3 years, 2 months ago

Selected Answer: A

Correct. Ans A.
Provide granular access to secrets: 2.Enforce access control to secrets using project-level identity and Access Management (IAM) bindings.
Give you control over the rotation schedules for the encryption keys that wrap your secrets: 3. Use customer-managed encryption keys to encrypt secrets.
Maintain environment separation: 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

upvoted 13 times

mikesp 3 years, 1 month ago

It is possible to grant IAM bindind to secret-level which is more granular than project-level but considering that it is necessary to manage encryption keys life-cycle, then the answer is A due to C does not allow that.

upvoted 4 times

AzureDP900 2 years, 8 months ago

Yes , A is right

upvoted 1 times

Medofree Highly Voted 3 years, 2 months ago

None of the answers are correct, here is why :

➪ Provide granular access to secrets => 2. Enforce access control to secrets using secret-level (and not project-level)
➪ Give you control over the rotation schedules for the encryption keys that wrap your secrets => 3. Use customer-managed encryption keys to encrypt secrets.
➪ Maintain environment separation => 1. Use separate Google Cloud projects to store Production and Non-Production secrets
➪ Provide ease of management => 3. Use Google-managed encryption keys to encrypt secrets. (could be in contradiction with Give you control over the rotation schedules….)

It should be an E answer :

E. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using secret-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

upvoted 6 times

desertlotus1211 1 year, 11 months ago

That's Answer A....

upvoted 1 times

1209apl Most Recent 3 months, 1 week ago

Selected Answer: C

Agree with Medofree's comment, there is no right answer here.
However, option C looks like the closest due the granular access to secrets requirement and the ease of management requirement . Option A would grant identities access to all the secrets in the project, you might be able use other settings with project level IAM bindings to achieve it, but it won't be easy to manage.

upvoted 1 times

nah99 8 months, 1 week ago

Selected Answer: C

It's C, right? Answer A doesn't provide granular access. C still provides control over rotation, verify for yourself:

Go to GCP Console -> Secrets Manager -> Create Secret -> Select Google Managed Encryption Key -> Enable "Set rotation

period" and you will see the options

upvoted 1 times

glb2 1 year, 4 months ago

Selected Answer: C

I think C is correct.
Secrets granular management, separate projects and keys managements into google.

upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: C

For me this is answer C.
It provides granular access control at the secret level. Option A provides project-level IAM bindings and not secret level.
While it uses Google-managed keys (offering less control over rotation), it simplifies management and still maintains a good security posture.
It maintains environment separation by using different projects for Production and Non-Production.
Balances between ease of management and security, though slightly more complex due to separate projects.

upvoted 2 times

glb2 1 year, 4 months ago

I think the same.

upvoted 1 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: A

A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets.

upvoted 3 times