Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 187 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 187
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A service account key has been publicly exposed on multiple public code repositories. After reviewing the logs, you notice that the keys were used to generate short-lived credentials. You need to immediately remove access with the service account.

What should you do?

A. Delete the compromised service account.

B. Disable the compromised service account key.

C. Wait until the service account credentials expire automatically.

D. Rotate the compromised service account key.

Show Suggested Answer

by a190d62 at *Aug. 3, 2023, 12:21 p.m.*

Comments

Type your comment...

Submit

a190d62 Highly Voted 1 year, 12 months ago

Selected Answer: A

Normally you would just choose (D) to not break the business continuity. But in this case, when short-lived credentials are created you need to disable/delete service account (disabling service account key doesn't revoke short-lived credentials)

https://cloud.google.com/iam/docs/keys-disable-enable#disabling

upvoted 12 times

Pime13 Most Recent 7 months, 2 weeks ago

Selected Answer: A

Important: Disabling a service account key does not revoke short-lived credentials that were issued based on the key. To revoke a compromised short-lived credential, you must disable or delete the service account that the credential represents. If you do so, any workload that uses the service account will immediately lose access to your resources.

https://cloud.google.com/iam/docs/keys-disable-enable#disabling

upvoted 1 times

Zek 7 months, 3 weeks ago

Selected Answer: A

https://cloud.google.com/iam/docs/keys-disable-enable#disabling

Disabling a service account key does not revoke short-lived credentials that were issued based on the key. To revoke a compromised short-lived credential, you must disable or delete the service account that the credential represents.

upvoted 1 times

BPzen 8 months ago

Selected Answer: B

B. Update the perimeter with egressTo and set identityType to ANY_IDENTITY
What it does:
Updates the service perimeter to allow egress (outbound) traffic from the perimeter to the external Google Cloud project.
egressTo specifies the allowed external resource (e.g., the external project with the disk image).
identityType: ANY_IDENTITY allows any identity within the perimeter to make the request.
Why it's correct:
This is the correct way to allow resources in the perimeter to read from the external project while maintaining VPC Service Controls restrictions.
Highly suitable, as it enables access to the third-party disk image while adhering to VPC Service Controls.

upvoted 1 times

MoAk 7 months, 4 weeks ago

wrong Q bud.

upvoted 1 times

MoAk 8 months, 1 week ago

Selected Answer: A

As per https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys#code-repositories

upvoted 1 times

DattaHinge 10 months, 1 week ago

Selected Answer: B

Disabling the compromised service account key immediately prevents any further unauthorized access

upvoted 1 times

glb2 1 year, 4 months ago

Selected Answer: A

A. Delete the compromised service account

upvoted 1 times

CISSP987 1 year, 10 months ago

Selected Answer: B

The best answer is B. Disable the compromised service account key.

Disabling the compromised service account key will immediately revoke access to all resources that are using the key. This will prevent any further unauthorized access to your cloud environment.

A. Delete the compromised service account. Deleting the compromised service account will also revoke access to all resources that are using the account. However, this will also delete all of the data associated with the account. This may not be an option if you need to preserve the data.

upvoted 2 times

ArizonaClassics 1 year, 11 months ago

A. Delete the compromised service account: Deleting the service account will immediately revoke its access, but it may also break systems or services that depend on this service account. This is usually a last-resort measure and could be disruptive to services using the account legitimately.

upvoted 2 times

cyberpunk21 1 year, 11 months ago

Selected Answer: A

To revoke short-lived credentials service account, need to be deleted.

upvoted 2 times

ymkk 1 year, 11 months ago

Selected Answer: A

I choose option A.
Disabling a service account key does not revoke short-lived credentials that were issued based on the key. To revoke a compromised short-lived credential, must delete the service account that the credential represents. If you do so, any workload that uses the service account will immediately lose access to your resources.

upvoted 3 times

nah99 8 months, 1 week ago

Same warning is showed on delete page docs
https://cloud.google.com/iam/docs/keys-create-delete#deleting

upvoted 1 times

nah99 8 months, 1 week ago

nvm that's for deleting the key... so yeah option A

upvoted 1 times

akg001 1 year, 11 months ago

A- is correct.
https://cloud.google.com/iam/docs/keys-disable-enable#:~:text=Important%3A%20Disabling%20a%20service%20account,account%20that%20the%20credential%20represents.

upvoted 2 times

Sanjana2020 1 year, 12 months ago

Why not B?

upvoted 2 times

cyberpunk21 1 year, 11 months ago

disabling service account key doesn't revoke short-lived credentials

upvoted 3 times