EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 241 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 241
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You are developing a new application that uses exclusively Compute Engine VMs. Once a day, this application will execute five different batch jobs. Each of the batch jobs requires a dedicated set of permissions on Google Cloud resources outside of your application. You need to design a secure access concept for the batch jobs that adheres to the least-privilege principle.

What should you do?

A. 1. Create a general service account “g-sa” to orchestrate the batch jobs.
2. Create one service account per batch job ‘b-sa-[1-5]’. Grant only the permissions required to run the individual batch jobs to the service accounts and generate service account keys for each of these service accounts.
3. Store the service account keys in Secret Manager. Grant g-sa access to Secret Manager and run the batch jobs with the permissions of b-sa-[1-5].

B. 1. Create a general service account “g-sa” to execute the batch jobs.
2. Grant the permissions required to execute the batch jobs to g-sa.
3. Execute the batch jobs with the permissions granted to g-sa.

C. 1. Create a workload identity pool and configure workload identity pool providers for each batch job.
2. Assign the workload identity user role to each of the identities configured in the providers.
3. Create one service account per batch job “b-sa-[1-5]”, and grant only the permissions required to run the individual batch jobs to the service accounts.
4. Generate credential configuration files for each of the providers. Use these files to execute the batch jobs with the permissions of b-sa-[1-5].

D. 1. Create a general service account “g-sa” to orchestrate the batch jobs.
2. Create one service account per batch job “b-sa-[1-5]”, and grant only the permissions required to run the individual batch

2. Create one service account per batch job "b-sa-[1-5]", and grant only the permissions required to run the individual batch jobs to the service accounts.

3. Grant the Service Account Token Creator role to g-sa. Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the batch jobs with the permissions of b-sa-[1-5].

Show Suggested Answer

by MisterHairy at *Nov. 21, 2023, 11:07 p.m.*

Comments

Type your comment...

Submit

pfilourenco 1 year, 1 month ago

Selected Answer: D

D is correct.

upvoted 1 times

chaoslinux 1 year, 3 months ago

I picked D over B. "least privilege"

upvoted 1 times

TM19860801 1 year, 5 months ago

Which is correct, B or D?

upvoted 1 times

MisterHairy 1 year, 8 months ago

Selected Answer: D

The correct answer is D. 1. Create a general service account “g-sa” to orchestrate the batch jobs. 2. Create one service account per batch job “b-sa-[1-5]”, and grant only the permissions required to run the individual batch jobs to the service accounts. 3. Grant the Service Account Token Creator role to g-sa. Use g-sa to obtain short-lived access tokens for b-sa-[1-5] and to execute the batch jobs with the permissions of b-sa-[1-5].

This approach adheres to the principle of least privilege by ensuring that each batch job has only the permissions it needs to run. The general service account “g-sa” is used to orchestrate the batch jobs, and the Service Account Token Creator role allows it to obtain short-lived access tokens for the batch job service accounts “b-sa-[1-5]”. This setup allows the batch jobs to be executed with the permissions of the respective service accounts.

upvoted 4 times