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 192 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 192

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization is rolling out a new continuous integration and delivery (CI/CD) process to deploy infrastructure and applications in Google Cloud. Many teams will use their own instances of the CI/CD workflow. It will run on Google Kubernetes Engine (GKE). The CI/CD pipelines must be designed to securely access Google Cloud APIs.

What should you do?

A. 1. Create two service accounts, one for the infrastructure and one for the application deployment.
2. Use workload identities to let the pods run the two pipelines and authenticate with the service accounts.
3. Run the infrastructure and application pipelines in separate namespaces.

B. 1. Create a dedicated service account for the CI/CD pipelines.
2. Run the deployment pipelines in a dedicated nodes pool in the GKE cluster.
3. Use the service account that you created as identity for the nodes in the pool to authenticate to the Google Cloud APIs.

C. 1. Create individual service accounts for each deployment pipeline.
2. Add an identifier for the pipeline in the service account naming convention.
3. Ensure each pipeline runs on dedicated pods.
4. Use workload identity to map a deployment pipeline pod with a service account.

D. 1. Create service accounts for each deployment pipeline.
2. Generate private keys for the service accounts.
3. Securely store the private keys as Kubernetes secrets accessible only by the pods that run the specific deploy pipeline.

Show Suggested Answer

by pfilourenco at *Aug. 5, 2023, 6:41 a.m.*

Comments

Type your comment...

Submit

7f97f9f 5 months, 1 week ago

Selected Answer: C

A is a very strong option. Using separate service accounts for infrastructure and application deployments follows the principle of least privilege. Workload Identity is the recommended way to securely authenticate GKE pods with Google Cloud APIs. Separate namespaces add an extra layer of isolation.

However, C is the most secure and granular approach. Creating individual service accounts per pipeline follows the principle of least privilege. Workload Identity ensures secure authentication. This is the best answer.

upvoted 4 times

JohnDohertyDoe 7 months ago

Selected Answer: C

Granular permissions per deployment pipeline would allow you to separate permissions based on the application teams. Additionally you would want to avoid container escapes by ensuring each deployment runs in a different pod. While A makes it simpler, C is better.

upvoted 2 times

Andrei_Z 10 months, 4 weeks ago

Selected Answer: D

it is D

upvoted 1 times

espressoboy 10 months, 2 weeks ago

https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview#giving_pods_access_to_resources

upvoted 1 times

GCBC 10 months, 4 weeks ago

Selected Answer: A

Ans is A, 2 SAs - one for infra and one for deployment

upvoted 3 times

cyberpunk21 11 months, 1 week ago

Selected Answer: A

A is correct

upvoted 2 times

alkaloid 11 months, 4 weeks ago

I'll go with A.
https://cloud.google.com/kubernetes-engine/docs/concepts/security-overview#giving_pods_access_to_resources

upvoted 1 times

pfilourenco 11 months, 4 weeks ago

Selected Answer: A

A is the correct, use workload identities and separeted namesapaces.

upvoted 2 times