EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 247 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 247
Topic #: 1
[All Associate Cloud Engineer Questions]

Your company is moving its continuous integration and delivery (CI/CD) pipeline to Compute Engine instances. The pipeline will manage the entire cloud infrastructure through code. How can you ensure that the pipeline has appropriate permissions while your system is following security best practices?

A. • Attach a single service account to the compute instances.
• Add minimal rights to the service account.
• Allow the service account to impersonate a Cloud Identity user with elevated permissions to create, update, or delete resources.

B. • Add a step for human approval to the CI/CD pipeline before the execution of the infrastructure provisioning.
• Use the human approvals IAM account for the provisioning.

C. • Attach a single service account to the compute instances.
• Add all required Identity and Access Management (IAM) permissions to this service account to create, update, or delete resources.

D. • Create multiple service accounts, one for each pipeline with the appropriate minimal Identity and Access Management (IAM) permissions.
• Use a secret manager service to store the key files of the service accounts.
• Allow the CI/CD pipeline to request the appropriate secrets during the execution of the pipeline.

by KelvinToo at *Dec. 31, 2023, 6:54 p.m.*

Comments

Type your comment...

Submit

iooj 1 month, 1 week ago

It seems, you all just use chat gpt to get the answer. But did you even notice it says one they need to move only one pipeline?

upvoted 1 times

iooj 1 month, 1 week ago

By the way, chat gpt o1-preview says: that A is the answer

Principle of Least Privilege: By assigning minimal rights to the service account, you limit access to only what's necessary for regular operations.
Impersonation for Elevated Actions: Allowing the service account to impersonate a Cloud Identity user with elevated permissions ensures that higher-level permissions are used only when needed and are tightly controlled.
Security Best Practices: This approach avoids the use of long-lived credentials or storing service account keys, reducing potential security risks.

upvoted 2 times

PiperMe 7 months, 3 weeks ago

Selected Answer: D

Option D combines the principle of least privilege with granular permissions, secure credential management, and controlled access during pipeline execution.

upvoted 3 times

guru_ji 8 months, 1 week ago

Selected Answer: D

Options A and C both involve attaching a single service account to the compute instances, which goes against the principle of least privilege and increases the risk if that single account is compromised. Option B introduces human approval into the CI/CD pipeline, which could slow down the deployment process and might not be feasible for fully automated deployments. Therefore, option D is the most suitable choice for ensuring both security and efficiency in the CI/CD pipeline setup.

upvoted 3 times

Cynthia2023 9 months, 3 weeks ago

Selected Answer: D

Principle of Least Privilege: Creating separate service accounts for different aspects of your CI/CD pipeline allows you to adhere to the principle of least privilege. This means each service account is granted only the permissions necessary for its specific role in the pipeline.

Security and Organization: Using multiple service accounts makes it easier to manage permissions, track activities, and audit usage for specific tasks or components of your CI/CD process.

Secret Management: Storing the service account key files in a secret manager service (like Google Cloud Secret Manager) enhances security. This approach securely manages and accesses these keys, reducing the risk of unauthorized access or exposure.

Dynamic Access: Allowing the CI/CD pipeline to request the appropriate secrets during execution ensures that credentials are provided only when needed and aren't unnecessarily exposed or stored in less secure environments.

upvoted 2 times

Cynthia2023 9 months, 3 weeks ago

A. Single Service Account with Impersonation: While using a single service account with minimal rights and impersonation can work, it introduces complexity and might not offer the same level of granularity and security as multiple service accounts. Impersonation also adds an additional layer that needs to be securely managed.

upvoted 2 times

KelvinToo 9 months, 3 weeks ago

Selected Answer: D

ChatGPT says Option D,
By following this approach, you can ensure that your CI/CD pipeline has appropriate permissions while adhering to security

best practices, including the principle of least privilege and secure management of credentials.

upvoted 2 times