

 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 117 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 117

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You plan to deploy your cloud infrastructure using a CI/CD cluster hosted on Compute Engine. You want to minimize the risk of its credentials being stolen by a third party. What should you do?

- A. Create a dedicated Cloud Identity user account for the cluster. Use a strong self-hosted vault solution to store the user's temporary credentials.
- B. Create a dedicated Cloud Identity user account for the cluster. Enable the constraints/iam.disableServiceAccountCreation organization policy at the project level.
- C. Create a custom service account for the cluster. Enable the constraints/iam.disableServiceAccountKeyCreation organization policy at the project level.
- D. Create a custom service account for the cluster. Enable the constraints/iam.allowServiceAccountCredentialLifetimeExtension organization policy at the project level.

[Show Suggested Answer](#)

by  mT3 at May 19, 2022, 5:48 p.m.

Comments

Type your comment...

[Submit](#)



  **ExamQnA** Highly Voted  3 years, 2 months ago

Selected Answer: C

Disable service account key creation

You can use the `iam.disableServiceAccountKeyCreation` boolean constraint to disable the creation of new external service account keys. This allows you to control the use of unmanaged long-term credentials for service accounts. When this constraint is set, user-managed credentials cannot be created for service accounts in projects affected by the constraint. https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#example_policy_boolean_constraint

   upvoted 7 times

  **AzureDP900** 2 years, 8 months ago

Yes

C. Create a custom service account for the cluster. Enable the constraints/`iam.disableServiceAccountKeyCreation` organization policy at the project level


   upvoted 1 times

  **Zek** Most Recent  7 months, 3 weeks ago

Selected Answer: C

C. Create a custom service account for the cluster. Enable the constraints/`iam.disableServiceAccountKeyCreation` organization policy at the project level

   upvoted 1 times

  **Xoxoo** 1 year, 10 months ago

Selected Answer: C

To minimize the risk of credentials being stolen by a third party when deploying your cloud infrastructure using a CI/CD cluster hosted on Compute Engine, you should create a custom service account for the cluster and enable the constraints/`iam.disableServiceAccountKeyCreation` organization policy at the project level.

By creating a custom service account for the cluster, you can have more control over the permissions and access granted to the cluster. This allows you to follow the principle of least privilege and ensure that only the necessary permissions are assigned to the service account.

Enabling the constraints/`iam.disableServiceAccountKeyCreation` organization policy at the project level helps prevent unauthorized access to the service account's credentials by disabling the creation of new service account keys.

   upvoted 1 times

  **[Removed]** 2 years ago

Selected Answer: C

"C"

Service Account Keys get exported outside GCP to local machines and this is where the main risk comes from. Therefore you can mitigate this risk by disabling the creation of service account keys.

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#disable_service_account_key_creation

   upvoted 2 times

  **mikesp** 3 years, 1 month ago

Selected Answer: C

Also think it is C

   upvoted 4 times

  **mT3** 3 years, 2 months ago

Selected Answer: C

Answer is (C).

To minimize the risk of credentials being stolen by third parties, it is desirable to control the use of unmanaged long-term credentials.

`"constraints/iam.allowServiceAccountCredentialLifetimeExtension"`: to extend the lifetime of the access token.

`"iam.disableServiceAccountCreation"`: Disables service account creation.

`"iam.disableServiceAccountCreation"`: Controls the use of unmanaged long-term credentials for service accounts.

Ref : https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#example_policy_boolean_constraint

   upvoted 2 times



Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

