Google Discussions

Exam Associate Cloud Engineer All Questions

View all questions & answers for the Associate Cloud Engineer exam

Go to Exam

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 70 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer

Question #: 70

Topic #: 1

[All Associate Cloud Engineer Questions]

You are building an application that will run in your data center. The application will use Google Cloud Platform (GCP) services like AutoML. You created a service account that has appropriate access to AutoML. You need to enable authentication to the APIs from your on-premises environment. What should you do?

A. Use service account credentials in your on-premises application.

B. Use gcloud to create a key file for the service account that has appropriate permissions.

C. Set up direct interconnect between your data center and Google Cloud Platform to enable authentication for your on-premises applications.

D. Go to the IAM & admin console, grant a user account permissions similar to the service account permissions, and use this user account for authentication from your data center.

Show Suggested Answer

by AS007 at *June 29, 2020, 5:14 a.m.*

Comments

Type your comment...

Submit

ESP_SAP Highly Voted 4 years, 2 months ago

Correct answer should be (B):

To use a service account outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal.

https://cloud.google.com/iam/docs/creating-managing-service-account-keys

upvoted 53 times

Buruguduystunstugudunstuy Highly Voted 1 year, 8 months ago

Selected Answer: B

The recommended approach for enabling authentication from an on-premises environment to Google Cloud Platform (GCP) services like AutoML is to use a service account and generate a JSON key file for the service account. This key file can then be used to authenticate and authorize API calls from your on-premises environment to GCP.

Therefore, the correct answer is B. Use gcloud to create a key file for the service account that has appropriate permissions.

upvoted 6 times

thewalker Most Recent 11 months ago

Selected Answer: B

B

As per the documentation: https://cloud.google.com/iam/docs/keys-create-delete#creating

upvoted 4 times

BAofBK 11 months, 2 weeks ago

The correct answer is B

upvoted 1 times

drinkwater 1 year ago

A. Use service account credentials in your on-premises application.

Explanation:

Service accounts are the recommended way to authenticate your application and authorize it to access GCP services. You can create and use service account credentials to authenticate your application running in your on-premises environment and access GCP services like AutoML.

Option B (using gcloud to create a key file for the service account) is a valid approach to generate credentials for a service account, but using those credentials in your application is essential, which aligns with option A.

Options C and D are not directly related to enabling authentication for on-premises applications using service account credentials. Setting up direct interconnect (option C) is about networking, and granting permissions to a user account (option D) is not the standard approach for authenticating an application running on-premises to GCP services

upvoted 1 times

Captain1212 1 year, 1 month ago

Selected Answer: B

B is the correct answer, as to access the out side the google cloud , you need the key

upvoted 1 times

Bobbybash 1 year, 8 months ago

Selected Answer: A

A. Use service account credentials in your on-premises application.

To enable authentication to GCP services from your on-premises environment, you can use service account credentials in your on-premises application. This involves creating a service account that has appropriate access to the required GCP services, downloading the service account key file, and using the key file to authenticate the API requests in your on-premises application. This is a secure way to authenticate to GCP services as it does not require direct access to your GCP project or credentials from your on-premises environment.

upvoted 2 times

Buruguduystunstugudunstuy 1 year, 8 months ago

Cloud Security/Auditor doesn't like Answer "A". Using service account credentials in your on-premises application could be a security risk if the credentials are compromised. If the key file is stolen or leaked, an attacker could use it to access your GCP resources, potentially causing data breaches, service disruptions, or financial losses.

I would select Answer "B". Use gcloud to create a key file for the service account that has appropriate permissions and let Security Auditor stay away from my back. Never-ending "You cannot do this, you cannot do that" on Answer A.

upvoted 3 times

upvoted 3 times

cslince 1 year, 10 months ago

Selected Answer: B

B it is.

upvoted 1 times

mvk2022 1 year, 10 months ago

Selected Answer: B

B it is.

upvoted 1 times

Kopy 1 year, 11 months ago

Selected Answer: B

Correct answer should be (B):

upvoted 1 times

AzureDP900 2 years, 4 months ago

B is right
To use a service account from outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. When you create a service account key, the public portion is stored on Google Cloud, while the private portion is available only to you. For more information about public/private key pairs, see Service account keys.

upvoted 4 times

haroldbenites 2 years, 4 months ago

Go for B

upvoted 1 times

NoniGeorge 2 years, 9 months ago

Selected Answer: B

Even thought A and B seem to be doing the same thing the best practice is to create a key so B is the right answer
!

upvoted 1 times

vishnukumartr 2 years, 11 months ago

B. Use gcloud to create a key file for the service account that has appropriate permissions.

upvoted 3 times

shawnkkk 2 years, 11 months ago

B. Use gcloud to create a key file for the service account that has appropriate permissions.

upvoted 3 times

Vivekvkt123 3 years ago

Why not A? Aren't A and B getting the same key file?

upvoted 3 times

jabrrJ68w02ond1 2 years, 11 months ago

A is not really telling you the steps to accomplish the task, it's only telling you the result of it (creating a SA with sufficient permissions and then use Console / gcloud to create a JSON token for it)

upvoted 1 times

sunilw 3 years, 3 months ago

B is correct.

Creating service account keys
To use a service account from outside of Google Cloud, such as on other platforms or on-premises, you must first establish the identity of the service account. Public/private key pairs provide a secure way of accomplishing this goal. When you create a service account key, the public portion is stored on Google Cloud, while the private portion is available only to you. For more information about public/private key pairs, see Service account keys.

upvoted 3 times

Load full discussion...

Social Media

Facebook , Twitter

YouTube , Reddit

Pinterest

We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.