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 134 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 134
Topic #: 1
[All Associate Cloud Engineer Questions]

You built an application on your development laptop that uses Google Cloud services. Your application uses Application Default Credentials for authentication and works fine on your development laptop. You want to migrate this application to a Compute Engine virtual machine (VM) and set up authentication using Google- recommended practices and minimal changes. What should you do?

A. Assign appropriate access for Google services to the service account used by the Compute Engine VM.

B. Create a service account with appropriate access for Google services, and configure the application to use this account.

C. Store credentials for service accounts with appropriate access for Google services in a config file, and deploy this config file with your application.

D. Store credentials for your user account with appropriate access for Google services in a config file, and deploy this config file with your application.

Show Suggested Answer

by filco72 at *Aug. 11, 2020, 2:01 p.m.*

Comments

Type your comment...

Submit

ESP_SAP Highly Voted 4 years, 2 months ago

Correct Answer is (B):

Best practices
In general, Google recommends that each instance that needs to call a Google API should run as a service account with the minimum permissions necessary for that instance to do its job. In practice, this means you should configure service accounts for your instances with the following process:

Create a new service account rather than using the Compute Engine default service account.
Grant IAM roles to that service account for only the resources that it needs.
Configure the instance to run as that service account.
Grant the instance the https://www.googleapis.com/auth/cloud-platform scope to allow full access to all Google Cloud APIs, so that the IAM permissions of the instance are completely determined by the IAM roles of the service account.
Avoid granting more access than necessary and regularly check your service account permissions to make sure they are up-to-date.

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#best_practices

upvoted 54 times

Ridhanya 2 years, 10 months ago

you just gave justification for option A which is right

upvoted 1 times

ryumada 2 years, 2 months ago

Maybe for the option A you are modifying the default service account because it's not explain which service account used by the VM, is it the default one or the new one?

The best practice is to Create a new service account rather than using the Compute Engine default service account.

B still has the bigger prove here as the answer.

upvoted 5 times

ryumada 2 years, 2 months ago

You should read lxgywil comment. His comment explains how authentication works to access Google Services in your application.

a relevant link also:
https://cloud.google.com/storage/docs/reference/libraries#setting_up_authentication

upvoted 1 times

cRobert 3 years, 10 months ago

From your quote:
Configure the "instance" to run as that service account.
From answer B:
and configure the "application" to use this account.

You don't add service accounts to applications, ans A

upvoted 20 times

magistrum 3 years, 9 months ago

wording is the clue :)

upvoted 1 times

TAvenger 3 years, 8 months ago

It's dirty play with words... All understand that we need custom SA, grant required permissions and attach this SA to the VM...
Why Google does this?

upvoted 7 times

lxgywil 3 years, 5 months ago

When you use a GCP service within your app (code), you have to use its client libraries. When you instantiate a client with client libraries you can pass it a Service Account key, which will define on behalf of which SA the client will be acting. That's how you can configure your app to use a particular service account.

E.g. https://cloud.google.com/storage/docs/reference/libraries#using_the_client_library

upvoted 3 times

akshaydoifode88 1 year, 11 months ago

In question it's written application uses application default credentials. So taking that as a hint. B is the answer because here we are configuring service account key into the application. Similar approach.

upvoted 1 times

filco72 Highly Voted 4 years, 2 months ago

I would choose: A. Assign appropriate access for Google services to the service account used by the Compute Engine VM. as there is no need to create a new service account.

upvoted 20 times

Hjameel 4 years, 2 months ago

I agree, there is no need to create a new service account

upvoted 9 times

xaqanik 1 year, 8 months ago

by default a vm uses a default service account. if you grant permission to this service account it will apply to all VMs default service accounts in the project . in this case you need create a new service account and give it appropriate permission

upvoted 6 times

denno22 Most Recent 3 weeks ago

Selected Answer: B

Create a new user-managed service account rather than using the Compute Engine default service account, and grant IAM roles to that service account for only the resources and operations that it needs.

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances#best_practices

upvoted 1 times

AchourOussama 1 month ago

I think the "minimal changes" hint here would make the first option the more suitable one since it doesn't involve creating a new service account.

upvoted 1 times

ccpmad 4 months, 4 weeks ago

Selected Answer: A

Is not possible to add the service accounts to the application

upvoted 1 times

pzacariasf7 7 months, 1 week ago

Selected Answer: B

B is the answer

upvoted 1 times

PiperMe 7 months, 3 weeks ago

I'd strongly lean towards Option B (Create a service account with appropriate access for Google services and configure the application to use this account) as the most likely correct answer.

Google's exams emphasize secure design principles. The principle of least privilege is a core tenet, and custom service accounts embody this. Option B aligns precisely with the best practice for production environments and demonstrates a clear understanding of IAM concepts. While Option A could be acceptable with careful permission adjustments, exams often favor the solution most demonstrably secure and aligned with recommended practice out of the box.
I believe option A might be a trap. Default service accounts can have varying levels of access. The exam might purposely use this ambiguity to test your knowledge of security principles. Focusing on the step of creating a custom service account signals your understanding of the correct IAM workflow.

upvoted 3 times

Cynthia2023 9 months, 3 weeks ago

Selected Answer: B

When you create a new Compute Engine VM, it is assigned a default service account, but this default service account is not unique to each VM. Instead, it's a project-wide default service account.
1. Project-Wide Default Service Account:
• The default service account is typically named something like PROJECT_NUMBER-compute@developer.gserviceaccount.com. It is the same across all VMs in the project that use the default service account.
• Permissions granted to this default service account apply to all VMs using this account, which could lead to potential security risks if not managed carefully, especially in projects with multiple VMs having different access requirements.

upvoted 3 times

Cynthia2023 9 months, 3 weeks ago

2. Creating a New Service Account:

• For better security and to adhere to the principle of least privilege, it's often recommended to create a new service account with just the necessary permissions for your specific application or VM.
• This approach allows for more granular control over permissions and reduces the risk of inadvertently granting excessive privileges to all VMs using the default service account.

upvoted 2 times

Cynthia2023 9 months, 3 weeks ago

Selected Answer: A

When you run an application on a Compute Engine VM, the VM can use a service account to interact with Google Cloud services. This service account is attached to the VM and can be used to authenticate your application without needing to explicitly manage credentials.

• B. Configure the application to use a new service account: While this is a viable approach, it requires more changes to your application to explicitly use a new service account. Using the VM's service account with ADC requires fewer changes.

upvoted 1 times

roy_02 10 months, 2 weeks ago

Selected Answer: B

B as option A is all about using default service account
whereas option B is to make new custom service account Google recommended .

upvoted 2 times

Sxn 11 months, 1 week ago

Selected Answer: B

By creating a service account, you can assign appropriate permissions for Google services to the service account and configure your application to use it. This way, your application can access Google services securely without having to store any user credentials or access tokens on the VM.
source1:https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances
source2: https://www.exam-answer.com/migrate-application-google-cloud-compute-engine-seo-friendly

upvoted 1 times

VijKall 11 months, 3 weeks ago

Selected Answer: B

I will go with B, by creating new SA and not by A , as SA used by the Compute Engine VM is by first choice a default SA and not user managed SA.

upvoted 1 times

Captain1212 1 year, 1 month ago

Selected Answer: A

A is the right answer , as after providing the appropriate access to the service account compute Engine

upvoted 1 times

MilanRajGupta 1 year, 2 months ago

The correct answer is "B". In general, Google recommends that each instance that needs to call a Google API should run as a service
account with the minimum permissions necessary for that instance to do its job. In practice, this means you should configure service accounts for your instances with the following process: Create a new service account rather than using the Compute Engine default service account. Grant IAM roles to that service account for only the resources that it needs. Configure the instance to run as that service account. Grant the instance the https://www.googleapis.com/auth/cloud-platform scope to allow full access to all Google Cloud APIs, so that the IAM permissions of the instance are completely determined by the IAM roles of the service account. Avoid granting more access than necessary and regularly check your service account permissions to make sure they are up-to-date.

upvoted 1 times

3arle 1 year, 2 months ago

B
"Many of these Google Cloud services also provide a default service account. Using the default service account is not recommended, because by default the default service account is highly privileged, which violates the principle of least privilege."
https://cloud.google.com/docs/authentication/provide-credentials-adc#attached-sa

upvoted 2 times

krop 1 year, 4 months ago

Selected Answer: A

Based on the documentation here : https://cloud.google.com/docs/authentication/application-default-credentials looks like the correct answer is "A".

This is exactly why ADC has been created for. You develop your code on your laptop and you using in your APP code ADC as a way to authorize to GCP - then depends on where you would like to test your code on - you simply execute `gcloud

auth application-default login` in your system to store right credentials in your ADC on your laptop.

When you copy your code into PROD VM, your app without any changes will scan below locations in order to find credentials :
1. GOOGLE_APPLICATION_CREDENTIALS environment variable
2. User credentials set up by using the Google Cloud CLI
3. The attached service account, returned by the metadata server

As you can see above, your app will not find any credentials in 1. and 2. location but it will go to location 3, which is the credential for Service Account assigned to your VM.

Minimal effort here means, you don't need to change your APP to get right credentials to GCP services.

upvoted 2 times

geeroylenkins 1 year, 3 months ago

This seems the best answer. Using ADC enables the App itself to use the VM's SA after migration. No change to the app is needed.

upvoted 1 times

eez64480 1 year, 5 months ago

Correct answer is A

Application Default Credentials (ADC) is not a declaration of permissions, but more of a directive to find permissions already granted to the application's environment.

Referencing the link below, you could certainly perform answer B, but the question specifies "minimal changes". We assign appropriate permissions to the instance that will be running the application and the ADC will find them and use them to authenticate. Kind of dumps the permissions responsibility on the cloud engineer to make sure the instance has the proper permissions.

https://google-auth.readthedocs.io/en/master/user-guide.html#application-default:~:text=Applications%20running%20on,compute_engine.Credentials%3A

upvoted 1 times

Load full discussion...