EXAMTOPICS

- Expert Verified, Online, Free.

≡ MENU   🔍

← 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 71 DISCUSSION**

Actual exam question from Google's Associate Cloud Engineer

Question #: 71

Topic #: 1

[All Associate Cloud Engineer Questions]

You are using Container Registry to centrally store your company's container images in a separate project. In another project, you want to create a Google

Kubernetes Engine (GKE) cluster. You want to ensure that Kubernetes can download images from Container Registry. What should you do?

    A. In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

    B. When you create the GKE cluster, choose the Allow full access to all Cloud APIs option under 'Access scopes'.

    C. Create a service account, and give it access to Cloud Storage. Create a P12 key for this service account and use it as an imagePullSecrets in Kubernetes.

    D. Configure the ACLs on each image in Cloud Storage to give read-only access to the default Compute Engine service account.

Show Suggested Answer

---

by [deleted] at *June 5, 2020, 3:05 p.m.*

Comments

⊟ 👤 **ESP_SAP** `Highly Voted 👍` 4 years, 2 months ago

Correct Answer (A):
IAM permissions
IAM permissions determine who can access resources. All users, service accounts, and other identities that interact with Container Registry must have the appropriate Cloud Storage permissions.

By default, Google Cloud use default service accounts to interact with resources within the same project. For example, the Cloud Build service account can both push and pull images when Container Registry is in the same project.

You must configure or modify permissions yourself if:

You are using a service account in one project to access Container Registry in a different project
You are using a default service account with read-only access to storage, but you want to both pull and push images
You are using a custom service account to interact with Container Registry

https://cloud.google.com/container-registry/docs/access-control

👍 ↩ 🏳 upvoted 64 times

   ⊟ 👤 **[Removed]** 4 years, 1 month ago

   A is correct, practical implementation in video https://www.youtube.com/watch?v=R16z7Sjrkxs

   👍 ↩ 🏳 upvoted 11 times

⊟ 👤 **XRiddlerX** `Highly Voted 👍` 4 years, 2 months ago

A is correct...
Container Registry uses Cloud Storage buckets as the underlying storage for container images. You control access to your images by granting appropriate Cloud Storage permissions to a user, group, service account, or other identity.

If the service account needs to access Container Registry in another project, you must grant the required permissions in the project with Container Registry.

Reference:
https://cloud.google.com/container-registry/docs/access-control#permissions

👍 ↩ 🏳 upvoted 21 times

⊟ 👤 **Enamfrancis** `Most Recent ⊘` 4 weeks ago

`Selected Answer: A`

A is correct

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **omunoz** 5 months, 1 week ago

As per https://cloud.google.com/container-registry/docs/access-control.

Container Registry is deprecated and scheduled for shutdown. After May 15, 2024, Artifact Registry will host images for the gcr.io domain in Google Cloud projects without previous Container Registry usage. After March 18, 2025, Container Registry will be shut down.

Artifact Registry is the recommended service for container image storage and management on Google Cloud.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **Captain1212** 1 year, 1 month ago

`Selected Answer: A`

A is the correct answer , as granting this role allow to download the image

👍 ↩ 🏳 upvoted 2 times

⊟ 👤 **sakdip66** 1 year, 6 months ago

`Selected Answer: A`

Grating Storage Object Viewer IAM Role to the service account used by Kubernetes nodes allow the nodes to download the images from Container registry.

👍 ↩ 🏳 upvoted 1 times

⊟ 👤 **Buruguduystunstugudunstuy** 1 year, 8 months ago

`Selected Answer: A`

Answer A. In the project where the images are stored, grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes.

To ensure that Kubernetes can download container images from Container Registry, you need to grant the necessary permissions to the service account used by the Kubernetes nodes. In this case, you would need to grant the Storage Object Viewer IAM role to the service account used by the Kubernetes nodes in the project where the images are stored. This role allows the service account to read objects from Cloud Storage buckets, including the container images in Container Registry.

👍 ↩ ⚑ upvoted 5 times

──────────

⊟ 👤 **jrisl1991** 1 year, 8 months ago

Selected Answer: A

Definitely A seems more practical and accurate.

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **GaneshSurwase** 2 years ago

CORRET ANS is A

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **ravip12345** 2 years, 1 month ago

Answer A is correct.
Storage Object Viewer (roles/storage.objectViewer) -- Grant the role on the registry storage bucket.
https://cloud.google.com/container-registry/docs/access-control

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **AzureDP900** 2 years, 4 months ago

Storage Object viewer is enough, A is right.

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **haroldbenites** 2 years, 4 months ago

Go for A.
the option A is specific with the role that will be used. In GCP , the recommendations is using the specific permission. The others options not are specific and are not correct .

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **somenick** 2 years, 7 months ago

Selected Answer: A

https://cloud.google.com/container-registry/docs/access-control

👍 ↩ ⚑ upvoted 2 times

──────────

⊟ 👤 **luciorifa** 2 years, 8 months ago

Selected Answer: A

A is the correct answe because it follows google recommended practices to grant permissions to service accounts, also the object viewer is the appropiate role for the GKE to pull the image

👍 ↩ ⚑ upvoted 2 times

──────────

⊟ 👤 **jdx000** 2 years, 8 months ago

Selected Answer: A

A is the most obvious

👍 ↩ ⚑ upvoted 1 times

──────────

⊟ 👤 **ArunTaneja** 2 years, 8 months ago

A should be correct
https://cloud.google.com/container-registry/docs/pushing-and-pulling#pulling_images_from_a_registry
https://cloud.google.com/storage/docs/access-control/iam-roles#standard-roles

👍 ↩ ⚑ upvoted 2 times

──────────

⊟ 👤 **NoniGeorge** 2 years, 9 months ago

It's A as you need Storage Object Viewer IAM role in order to have access to the images!

👍 ↩ ⚑ upvoted 1 times

Load full discussion...

👥

Social Media

Facebook , Twitter
YouTube , Reddit
Pinterest

EXAMTOPICS

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.

f t ▶ ⊙ ⊙