Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions*

Service Accounts

Question: What are the advantages of using service account impersonation to create short-lived tokens?

A. Short-lived credentials have a limited lifetime, with durations of just a few hours or shorter, and are not automatically refreshed.
B. They create less risk than long-lived credentials, such as service account keys.
C. The short-lived tokens can be used indefinitely without any expiration.
D. The short-lived tokens can be used to grant unlimited access to all resources in the project.

Question: What is the role required to be granted to a service account to create short-lived credentials for another service account?

A. Service Account User role (roles/iam.serviceAccountUser)
B. Service Account Token Creator role (roles/iam.serviceAccountTokenCreator)
C. Service Account Admin role (roles/iam.serviceAccountAdmin)

Question: What is the maximum expiration time for a self-signed JSON Web Token (JWT) when calling a Google API?

A. 12 hours
B. 1 hour
C. 24 hours

Question: How can you grant a service account access to resources in another project? For example, you may have a Compute Engine VM in project A that needs “viewer” access to a Cloud Storage bucket in project B.

A. By creating the same service account in both projects and assigning the Storage Viewer role to both of them.
B. Create the service account in project A. Add the same service account as an Identity in project B. In project B, grant the service account the Storage Viewer role.
C. Create the service account in project B. Add the same service account as an Identity in project A. In project A, grant the service account the Storage Viewer role.
D. Create the service account in project A. Add the same service account as an Identity in project B. In project B, grant the service account the Storage Admin role

Answers to Quiz questions

Service Accounts

Question: What are the advantages of using service account impersonation to create short-lived tokens?

A. Short-lived credentials have a limited lifetime, with durations of just a few hours or shorter, and are not automatically refreshed.
B. They create less risk than long-lived credentials, such as service account keys.
C. The short-lived tokens can be used indefinitely without any expiration.
D. The short-lived tokens can be used to grant unlimited access to all resources in the project.

Answer: A and B
Reference: Create short-lived credentials for a service account

Question: What is the role required to be granted to a service account to create short-lived credentials for another service account?

A. Service Account User role (roles/iam.serviceAccountUser)
B. Service Account Token Creator role (roles/iam.serviceAccountTokenCreator)
C. Service Account Admin role (roles/iam.serviceAccountAdmin)

Answer: B
Reference: Create short-lived credentials for a service account

Question: What is the maximum expiration time for a self-signed JSON Web Token (JWT) when calling a Google API?

A. 12 hours
B. 1 hour

C. 24 hours

Answer: B
Reference: Create short-lived credentials for a service account

Question: How can you grant a service account access to resources in another project? For example, you may have a Compute Engine VM in project A that needs “viewer” access to a Cloud Storage bucket in project B.

A. By creating the same service account in both projects and assigning the Storage Viewer role to both of them.
B. Create the service account in project A. Add the same service account as an Identity in project B. In project B, grant the service account the Storage Viewer role.
C. Create the service account in project B. Add the same service account as an Identity in project A. In project A, grant the service account the Storage Viewer role.
D. Create the service account in project A. Add the same service account as an Identity in project B. In project B, grant the service account the Storage Admin role

Answer B.

Reference: Configure for a resource in a different project