1.

You are trying to assign roles to the dev and prod projects of Cymbal Superstore’s e-commerce app but are receiving an error when you try to run set-iam policy. The projects are organized into an ecommerce folder in the Cymbal Superstore organizational hierarchy. You want to follow best practices for the permissions you need while respecting the practice of least privilege. What should you do?

1. Ask your administrator for resourcemanager.projects.setIamPolicy roles for each project
2. Ask your administrator for the roles/iam.securityAdmin role in IAM.
3. Ask your administrator for the roles/resourcemanager.folderIamAdmin for the ecommerce folder
4. Ask your administrator for the roles/resourcemanager.organizationAdmin for Cymbal Superstore

Correct! This choice gives you the required permissions while minimizing the number of individual resources you have to set permissions for.

check

2.

You need to configure access to Cloud Spanner from the GKE cluster that is supporting Cymbal Superstore’s ecommerce microservices application. You want to specify an account type to set the proper permissions. What should you do?

1. Assign permissions to a Google account referenced by the application
2. Assign permissions through a Cloud Identity account referenced by the application
3. Assign permissions through a Google Workspace account referenced by the application
4. Assign permissions through service account referenced by the application

3.

Which of the scenarios below is an example of a situation where you should use a service account?

1. To directly access user data
2. For individual GKE pods
3. For development environments
4. For interactive analysis

4.

Cymbal Superstore is implementing a mobile app for end users to track deliveries that are en route to them. The app needs to access data about truck location from Pub/Sub using Google recommended practices. What kind of credentials should you use?

1. API key
2. Service account key
3. OAuth 2.0 client
4. Environment provided service account

5.

Which Cloud Audit log is disabled by default with a few exceptions?

1. Admin Activity audit logs
2. Policy Denied audit logs
3. Data Access audit logs
4. System Event audit logs

6.

You have a custom role implemented for administration of the dev/test environment for Cymbal Superstore’s transportation management application. You are developing a pilot to use Cloud Run instead of Cloud Functions. You want to ensure your administrators have the correct access to the new resources. What should you do?

1. Make the change to the custom role locally and run an update on the custom role
2. Create a new role with needed permissions and migrate users to it.
3. Delete the custom role and recreate a new custom role with required permissions
4. Copy the existing role, add the new permissions to the copy, and delete the old role

7.

Outline where Cloud Audit logs can be accessed: in the logging tab of the operations interface Link: <https://cloud.google.com/storage/docs/audit-logging> You are configuring audit logging for Cloud Storage. You want to know when objects are added to a bucket. Which type of audit log entry should you monitor?

1. Admin Activity log entries
2. DATA\_WRITE log entries
3. ADMIN\_READ log entries
4. DATA\_READ log entries