Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions: Cloud Storage Authentication*

** These are for practice only and are not actual exam questions*

Which of the following resources allows anonymous access in Cloud Storage?

a) Resources with the "private" ACL

b) Resources with the "authenticatedUsers" ACL

c) Resources with the "allUsers" ACL

d) Resources with the "authenticated" ACL

What is the primary authentication mechanism used in Cloud Storage for API access?

a) API keys
b) Basic Authentication
c) OAuth 2.0
d) HMAC authentication

In Cloud Storage, which type of authentication flow should be used when your application needs to access user data?

a) Server-centric flow
b) User-centric flow
c) HMAC flow
d) Basic Authentication flow

Which scope in OAuth 2.0 would allow an application to read and change data but not modify metadata like IAM policies in Cloud Storage?

a) read-only
b) read-write
c) full-control
d) cloud-platform.read-only

How can you authorize requests to Cloud Storage using OAuth 2.0 from the command line for local testing?

a) Use the gcloud auth application-default print-access-token command

b) Include the API key in the request header
c) Use HMAC authentication
d) Use Basic Authentication

Answers

Which of the following resources allows anonymous access in Cloud Storage?
(c) Resources with the "allUsers" ACL. A resource has anonymous access if the allUsers group is included in the ACL for the resource or if the allUsers group is included in an IAM policy that applies to the resource. The allUsers group includes anyone on the Internet.
https://cloud.google.com/storage/docs/authentication

What is the primary authentication mechanism used in Cloud Storage for API access?
(c) OAuth 2.0. Cloud Storage uses OAuth 2.0 for API authentication and authorization. Authentication is the process of determining the identity of a client.
https://cloud.google.com/storage/docs/authentication

In Cloud Storage, which type of authentication flow should be used when your application needs to access user data?

(b) User-centric flow. A user-centric flow allows an application to obtain credentials from an end user. The user signs in to complete authentication. Use this flow if your application needs to access user data. See the User account credentials section later in this page for scenarios where a user-centric flow is appropriate.
https://cloud.google.com/storage/docs/authentication

Which scope in OAuth 2.0 would allow an application to read and change data but not modify metadata like IAM policies in Cloud Storage?
(b) read-write. An application with an access token with read-write scope can read and modify data. *read-write* Allows access to read and change data, but not metadata like IAM policies.
https://cloud.google.com/storage/docs/authentication

How can you authorize requests to Cloud Storage using OAuth 2.0 from the command line for local testing?
(a) Use the gcloud auth application-default print-access-token command. For local testing, you can use the *gcloud auth application-default print-access-token* command to generate a token. https://cloud.google.com/storage/docs/authentication