Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions*

API Keys

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

Question: Which of the following is the recommended method for authenticating to Google Cloud services from a server-side application?

A. Using static API keys.
B. Using OAuth 2.0 with user consent.
C. Using application default credentials.
D. Using end-user session tokens.

Question: When should you use API keys for authentication in Google Cloud?

A. When accessing private resources.
B. When accessing resources that require user authentication.
C. When accessing Google Cloud services from client-side applications.

D. When accessing public APIs that don't require user identity.

Question: Which of the following is NOT a recommended practice for securing API keys in Google Cloud?

A. Storing them in Secret Manager.
B. Embedding them directly in client-side code.
C. Rotating them periodically.
D. Restricting them by IP address or service.

Question: Which Google Cloud service allows you to manage and rotate API keys and other secrets?

A. Cloud Key Management Service.
B. Secret Manager.
C. Cloud Identity.
D. Cloud Storage.

Question: When using API keys for authentication, which of the following headers is typically used to pass the key in an HTTP request?

A. Authorization
B. Bearer
C. API-Key
D. x-api-key

Question: Which of the following is a risk associated with using static API keys for authentication?

A. They can be easily rotated.
B. They can be embedded in client-side applications.
C. They can be exposed in public repositories or logs.

D. They are tied to a user's identity.

Question: In which scenario would you NOT use an API key for authentication in Google Cloud?

A. When accessing a public API.
B. When the identity of the calling application matters.
C. When accessing a service that doesn't require user identity.
D. When making a request from a client-side application.

Answers to Quiz questions

API Keys

Question: Which of the following is the recommended method for authenticating to Google Cloud services from a server-side application?

A. Using static API keys.
B. Using OAuth 2.0 with user consent.
C. Using application default credentials.
D. Using end-user session tokens.

Correct Answer: C. Using application default credentials.

Explanation: Application default credentials provide a seamless way to authenticate server-side applications running on Google Cloud.
Resource Link: Authenticating as a service account

Question: When should you use API keys for authentication in Google Cloud?

A. When accessing private resources.
B. When accessing resources that require user authentication.

C. When accessing Google Cloud services from client-side applications.
D. When accessing public APIs that don't require user identity.

Correct Answer: D. When accessing public APIs that don't require user identity.

Explanation: API keys are used for accessing APIs that are public and don't require user identity.
Resource Link: Using API keys

Question: Which of the following is NOT a recommended practice for securing API keys in Google Cloud?

A. Storing them in Secret Manager.
B. Embedding them directly in client-side code.
C. Rotating them periodically.
D. Restricting them by IP address or service.

Correct Answer: B. Embedding them directly in client-side code.

Explanation: Embedding API keys directly in client-side code exposes them to potential misuse. It's always recommended to keep them secure and not expose them publicly.
Resource Link: Best practices for securing API keys

Question: Which Google Cloud service allows you to manage and rotate API keys and other secrets?

A. Cloud Key Management Service.
B. Secret Manager.
C. Cloud Identity.
D. Cloud Storage.

Correct Answer: B. Secret Manager.

Explanation: Secret Manager is a Google Cloud service that allows you to store, manage, and rotate secrets including API keys.

Resource Link: Secret Manager Overview

Question: When using API keys for authentication, which of the following headers is typically used to pass the key in an HTTP request?

A. Authorization
B. Bearer
C. API-Key
D. x-api-key

Correct Answer: D. x-api-key

Explanation: While the exact header can vary based on the API, x-api-key is a common header used to pass API keys in HTTP requests.
Resource Link: API Key Authentication

Question: Which of the following is a risk associated with using static API keys for authentication?

A. They can be easily rotated.
B. They can be embedded in client-side applications.
C. They can be exposed in public repositories or logs.
D. They are tied to a user's identity.

Correct Answer: C. They can be exposed in public repositories or logs.

Explanation: Static API keys, if not managed properly, can be accidentally exposed in public places like repositories or logs, leading to potential misuse.
Resource Link: Keeping API keys safe

Question: In which scenario would you NOT use an API key for authentication in Google Cloud?

A. When accessing a public API.
B. When the identity of the calling application matters.
C. When accessing a service that doesn't require user identity.

D. When making a request from a client-side application.

Correct Answer: B. When the identity of the calling application matters.

Explanation: API keys don't provide identity. If the identity of the calling application is important, other authentication methods like OAuth tokens or service account keys should be used.
Resource Link: Choosing an authentication method