Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions*

Workload Identity

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

Question: In the context of Google Cloud, what does Workload Identity primarily enable?

A. It allows for the encryption of data at rest.
B. It provides a mechanism for applications to impersonate service accounts.
C. It is used for managing user sessions in a distributed environment.
D. It is a tool for monitoring network traffic in VPCs.

Question: Which Google Cloud service can be integrated with Workload Identity to manage service-to-service communications securely?

A. Google Cloud Storage
B. Google Cloud Functions

C. Service Mesh
D. Google Cloud Pub/Sub

Question: When using Workload Identity, which authentication method is commonly associated with service-to-service communication?

A. OAuth 2.0
B. JWT
C. SSL
D. mTLS

Question: Which of the following is NOT a primary use case for Workload Identity in Google Cloud?

A. Impersonating service accounts from external systems.
B. Encrypting data in Cloud Storage buckets.
C. Reducing the risk of service account key misuse.
D. Providing a mechanism for applications to access Google Cloud resources.

Question: For securing service-to-service communications in a Kubernetes environment, which combination would be most effective?

A. Workload Identity and Kubernetes Network Policies
B. Workload Identity and Google Cloud Storage
C. Google Cloud Pub/Sub and Service Mesh
D. Google Cloud Functions and Google Cloud Run

Question: When using Workload Identity, which of the following is a recommended practice for running services?

A. Running services with maximum privileges.

B. Using static API keys for authentication.
C. Running services with least privileged access.
D. Storing service account keys in public repositories.

Question: Which of the following Google Cloud services can be used to store, access, and rotate application secrets, and can be integrated with Workload Identity for secure access?

A. Google Cloud Pub/Sub
B. Google Cloud Storage
C. Secret Manager
D. Google Cloud Scheduler

Question: In a microservices environment on Google Kubernetes Engine (GKE), you want to ensure that your application can securely read/write data to a Cloud Spanner database. Which of the following is the recommended way to authenticate your application to Cloud Spanner?

A. Use static API keys stored in Kubernetes secrets.
B. Use Workload Identity to bind Kubernetes service accounts to Google Cloud service accounts.
C. Store service account JSON keys in a ConfigMap and mount it to the application.
D. Use OAuth 2.0 client credentials flow with user impersonation.

Question: In a GKE-based microservices application, you want to ensure that only specific microservices can read from or write to a Cloud Spanner database. Which of the following approaches should you adopt?

A. Use Network Policies in GKE to restrict access based on pod labels.
B. Assign the Cloud Spanner admin role to all microservices for unrestricted access.

C. Use Workload Identity and grant the necessary IAM roles only to the service account associated with specific microservices.
D. Store Cloud Spanner credentials in a shared volume and mount it to all microservices.

Question: You are deploying a microservices application on GKE that interacts with Cloud Spanner. To ensure high availability and fault tolerance, which of the following practices should you adopt?

A. Deploy the application in a single zone for reduced latency.
B. Use regional Cloud Spanner instances and deploy the GKE cluster across multiple zones.
C. Store Cloud Spanner credentials in environment variables.
D. Use Cloud Spanner's single-region instance and deploy the GKE cluster in a single zone.

Answers to Quiz questions

Workload Identity

Question: In the context of Google Cloud, what does Workload Identity primarily enable?

A. It allows for the encryption of data at rest.
B. It provides a mechanism for applications to impersonate service accounts.
C. It is used for managing user sessions in a distributed environment.
D. It is a tool for monitoring network traffic in VPCs.

Correct Answer: B. It provides a mechanism for applications to impersonate service accounts.

Explanation: Workload Identity is a modern way to provision application access to cloud resources without using traditional service account keys.
Resource Link: Workload Identity Documentation - Google Cloud

Question: Which Google Cloud service can be integrated with Workload Identity to manage service-to-service communications securely?

A. Google Cloud Storage
B. Google Cloud Functions
C. Service Mesh
D. Google Cloud Pub/Sub

Correct Answer: Service Mesh

Explanation: C. Service Mesh, especially when combined with Workload Identity, can provide secure service-to-service communications.
Resource Link: Service Mesh Documentation - Google Cloud

Question: When using Workload Identity, which authentication method is commonly associated with service-to-service communication?

A. OAuth 2.0
B. JWT
C. SSL
D. mTLS

Correct Answer: D. mTLS

Explanation: mTLS (mutual TLS) is a two-sided authentication that ensures traffic is both secure and trusted in both directions.
Resource Link: mTLS Authentication - Google Cloud

Question: Which of the following is NOT a primary use case for Workload Identity in Google Cloud?

A. Impersonating service accounts from external systems.

B. Encrypting data in Cloud Storage buckets.
C. Reducing the risk of service account key misuse.
D. Providing a mechanism for applications to access Google Cloud resources.

Correct Answer: B. Encrypting data in Cloud Storage buckets.

Explanation: Workload Identity does not handle encryption. Its primary use is for authentication and authorization.
Resource Link: Workload Identity Federation - Google Cloud

Question: For securing service-to-service communications in a Kubernetes environment, which combination would be most effective?

A. Workload Identity and Kubernetes Network Policies
B. Workload Identity and Google Cloud Storage
C. Google Cloud Pub/Sub and Service Mesh
D. Google Cloud Functions and Google Cloud Run

Correct Answer: A. Workload Identity and Kubernetes Network Policies

Explanation: Using Workload Identity for authentication combined with Kubernetes Network Policies for network segmentation provides a secure communication environment.
Resource Link: Kubernetes Network Policies - Google Cloud

Question: When using Workload Identity, which of the following is a recommended practice for running services?

A. Running services with maximum privileges.
B. Using static API keys for authentication.
C. Running services with least privileged access.
D. Storing service account keys in public repositories.

Correct Answer: C. Running services with least privileged access.

Explanation: It's a best practice to run services with the least privileges necessary to perform their tasks to reduce potential attack vectors.
Resource Link: Principle of Least Privilege

Question: Which of the following Google Cloud services can be used to store, access, and rotate application secrets, and can be integrated with Workload Identity for secure access?

A. Google Cloud Pub/Sub
B. Google Cloud Storage
C. Secret Manager
D. Google Cloud Scheduler

Correct Answer: C. Secret Manager

Explanation: Secret Manager is a dedicated service for handling application secrets. It can be integrated with Workload Identity for secure and authorized access.
Resource Link: Secret Manager Documentation - Google Cloud

Question: In a microservices environment on Google Kubernetes Engine (GKE), you want to ensure that your application can securely read/write data to a Cloud Spanner database. Which of the following is the recommended way to authenticate your application to Cloud Spanner?

A. Use static API keys stored in Kubernetes secrets.
B. Use Workload Identity to bind Kubernetes service accounts to Google Cloud service accounts.
C. Store service account JSON keys in a ConfigMap and mount it to the application.
D. Use OAuth 2.0 client credentials flow with user impersonation.

Correct Answer: B. Use Workload Identity to bind Kubernetes service accounts to Google Cloud service accounts.

Explanation: Workload Identity allows you to bind Kubernetes service accounts to Google Cloud service accounts. This way, your application can assume the identity of the Google Cloud service account when accessing Google Cloud resources, eliminating the need to manage service account keys.
Resource Link: Workload Identity documentation - Google Cloud

Question: In a GKE-based microservices application, you want to ensure that only specific microservices can read from or write to a Cloud Spanner database. Which of the following approaches should you adopt?

A. Use Network Policies in GKE to restrict access based on pod labels.
B. Assign the Cloud Spanner admin role to all microservices for unrestricted access.
C. Use Workload Identity and grant the necessary IAM roles only to the service account associated with specific microservices.
D. Store Cloud Spanner credentials in a shared volume and mount it to all microservices.

Correct Answer: C. Use Workload Identity and grant the necessary IAM roles only to the service account associated with specific microservices.

Explanation: By using Workload Identity, you can bind specific Kubernetes service accounts to Google Cloud service accounts. You can then grant the necessary Cloud Spanner IAM roles only to those Google Cloud service accounts associated with specific microservices, ensuring fine-grained access control.
Resource Link:Connect Cloud Spanner with a Google Kubernetes Engine (GKE) cluster

Question: You are deploying a microservices application on GKE that interacts with Cloud Spanner. To ensure high availability and fault tolerance, which of the following practices should you adopt?

A. Deploy the application in a single zone for reduced latency.
B. Use regional Cloud Spanner instances and deploy the GKE cluster across multiple zones.
C. Store Cloud Spanner credentials in environment variables.

D. Use Cloud Spanner's single-region instance and deploy the GKE cluster in a single zone.

Correct Answer: B. Use regional Cloud Spanner instances and deploy the GKE cluster across multiple zones.

Explanation: Using regional Cloud Spanner instances ensures that your database is available across multiple zones, providing high availability. Similarly, deploying your GKE cluster across multiple zones ensures that your application remains available even if one zone fails.
Resource Link: GKE best practices: Designing and building highly available clusters