Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions*

Workload Identity Federation

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

Question: Which of the following describes the primary purpose of Workload Identity Federation in Google Cloud?

A. To enable A/testing for Google Cloud services.
B. To allow workloads running outside Google Cloud to impersonate a service account.
C. To manage Google Cloud resources using static API keys.
D. To provide SSL and mTLS authentication for Google Cloud services.

Question: When integrating workload identity federation with other cloud providers like AWS or Azure, which of the following is a key step?

A. Creating a static API key in Google Cloud.
B. Using Google Cloud's OAuth 2.0 token exchange protocol.

C. Implementing A/testing strategies for workload identity.
D. Using Google Cloud Debugger for application troubleshooting.

Question: For workloads running outside of Google Cloud, how can they access microservices hosted by Cloud Run using workload identity federation?

A. By using Google Cloud's Secret Manager.
B. By implementing Google Cloud's A/testing strategies.
C. By using credentials from an external identity provider.
D. By using Google Cloud's SSL and mTLS authentication.

Question: Which identity providers can be used with Workload Identity Federation?

A. Only Google Cloud Identity.
B. AWS, Azure Active Directory, and any IdP that supports OpenIConnect (OIDC) or SAML 2.0.
C. Only AWS and Azure.
D. Only on-premises Active Directory.

Question: What is the primary security advantage of using Workload Identity Federation over traditional service account keys?

A. It allows for unlimited access to all Google Cloud resources.
B. It eliminates the maintenance and security burden associated with service account keys.
C. It provides a static API key for all services.
D. It enforces two-factor authentication for all services.

Question: Which of the following is NOT a recommended best practice when implementing Workload Identity Federation?

A. Minimizing the use of service account keys.
B. Granting broad permissions to the federated workload.
C. Regularly rotating and revoking external identities.
D. Using attribute conditions to enforce token constraints.

Question: In the context of using Workload Identity Federation with GitHub Actions, which Google Cloud service can be used to exchange GitHub's OIDC tokens for Google-issued tokens?

A. Google Cloud Storage.
B. Google Cloud Identity Platform.
C. Google Cloud Token Service.
D. Google Cloud Pub/Sub.

Answers to Quiz questions

Workload Identity Federation

Question: Which of the following describes the primary purpose of Workload Identity Federation in Google Cloud?

A. To enable A/testing for Google Cloud services.
B. To allow workloads running outside Google Cloud to impersonate a service account.
C. To manage Google Cloud resources using static API keys.
D. To provide SSL and mTLS authentication for Google Cloud services.

Correct Answer: B. To allow workloads running outside Google Cloud to impersonate a service account.
Explanation: Workload identity federation lets applications running outside Google Cloud impersonate a service account, improving security and authentication mechanisms.

Resource Link: Best practices for using workload identity federation - Google Cloud

Question: When integrating workload identity federation with other cloud providers like AWS or Azure, which of the following is a key step?

A. Creating a static API key in Google Cloud.
B. Using Google Cloud's OAuth 2.0 token exchange protocol.
C. Implementing A/testing strategies for workload identity.
D. Using Google Cloud Debugger for application troubleshooting.

Correct Answer: B. Using Google Cloud's OAuth 2.0 token exchange protocol.
Explanation: Workload identity federation follows the OAuth 2.0 token exchange protocol to allow external workloads to authenticate to Google Cloud.

Resource Link: Configure workload identity federation with AWS or Azure - Google Cloud

Question: For workloads running outside of Google Cloud, how can they access microservices hosted by Cloud Run using workload identity federation?

A. By using Google Cloud's Secret Manager.
B. By implementing Google Cloud's A/testing strategies.
C. By using credentials from an external identity provider.
D. By using Google Cloud's SSL and mTLS authentication.

Correct Answer: C. By using credentials from an external identity provider.
Explanation: Workload identity federation allows external workloads to use credentials from an external identity provider to access Google Cloud services like Cloud Run.

Resource Link: Integrate Cloud Run and workload identity federation

Question: Which identity providers can be used with Workload Identity Federation?

A. Only Google Cloud Identity.
B. AWS, Azure Active Directory, and any IdP that supports OpenIConnect (OIDC) or SAML 2.0.
C. Only AWS and Azure.
D. Only on-premises Active Directory.

Correct Answer: B. AWS, Azure Active Directory, and any IdP that supports OpenIConnect (OIDC) or SAML 2.0.
Explanation: Workload Identity Federation supports AWS, Azure Active Directory, and any identity provider (IdP) that supports OpenIConnect (OIDC) or SAML 2.0.

Resource Link: Workload identity federation

Question: What is the primary security advantage of using Workload Identity Federation over traditional service account keys?

A. It allows for unlimited access to all Google Cloud resources.
B. It eliminates the maintenance and security burden associated with service account keys.
C. It provides a static API key for all services.
D. It enforces two-factor authentication for all services.

Correct Answer: B. It eliminates the maintenance and security burden associated with service account keys.
Explanation: With identity federation, external identities can be granted IAM roles, including the ability to impersonate service accounts. This approach eliminates the need for managing service account keys, which can be a security risk if not handled correctly.

Resource Link: Why use identity federation? - Google Cloud

Question: Which of the following is NOT a recommended best practice when implementing Workload Identity Federation?

A. Minimizing the use of service account keys.
B. Granting broad permissions to the federated workload.
C. Regularly rotating and revoking external identities.
D. Using attribute conditions to enforce token constraints.

Correct Answer: B. Granting broad permissions to the federated workload.
Explanation: It's always recommended to follow the principle of least privilege. Granting broad permissions increases the risk of unauthorized access or actions.

Resource Link: Best practices for using workload identity federation

Question: In the context of using Workload Identity Federation with GitHub Actions, which Google Cloud service can be used to exchange GitHub's OIDC tokens for Google-issued tokens?

A. Google Cloud Storage.
B. Google Cloud Identity Platform.
C. Google Cloud Token Service.
D. Google Cloud Pub/Sub.

Correct Answer: C. Google Cloud Token Service.
Explanation: Google Cloud Token Service is responsible for exchanging tokens from external identity providers, like GitHub's OIDC tokens, for Google-issued tokens, facilitating the authentication process in Workload Identity Federation.

Resource Link: Enabling keyless authentication from GitHub Actions

Question: Which of the following describes the primary purpose of Workload Identity Federation in Google Cloud?

- To enable A/testing for Google Cloud services.
- To allow workloads running outside Google Cloud to impersonate a service account.

- To manage Google Cloud resources using static API keys.
- To provide SSL and mTLS authentication for Google Cloud services.

Correct Answer: B. To allow workloads running outside Google Cloud to impersonate a service account.
Explanation: Workload identity federation lets applications running outside Google Cloud impersonate a service account, improving security and authentication mechanisms.

Resource Link: Best practices for using workload identity federation - Google Cloud