PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

You want to use the gcloud command-line tool to authenticate using a third-party single sign-on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)

A. SSO SAML as a third-party IdP

B. Identity Platform

C. OpenID Connect

D. Identity-Aware Proxy

E. Cloud Identity

Correct Answer: AC

To provide users with SSO-based access to selected cloud apps, Cloud Identity as your IdP supports the OpenID Connect (OIDC) and Security Assertion Markup Language 2.0 (SAML) protocols. https:// cloud.google.com/identity/solutions/ enable-sso

QUESTION 2

An organization is moving applications to Google Cloud while maintaining a few mission-critical applications on-premises. The organization must transfer the data at a bandwidth of at least 50 Gbps. What should they use to ensure secure continued connectivity between sites?

A. Dedicated Interconnect

B. Cloud Router

C. Cloud VPN

D. Partner Interconnect

Correct Answer: A

Reference: https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large- datasets https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview

QUESTION 3

You run applications on Cloud Run. You already enabled container analysis for vulnerability scanning. However, you are concerned about the lack of control on the applications that are deployed. You must ensure that only trusted container images are deployed on Cloud Run.

What should you do? Choose 2 answers

A. Enable Binary Authorization on the existing Kubernetes cluster.

B. Set the organization policy constraint constraints/run. allowedBinaryAuthorizationPolicie to the list of allowed Binary Authorization policy names.

C. Set the organization policy constraint constraints/compute.trustedimageProjects to the list of protects that contain the trusted container images.

D. Enable Binary Authorization on the existing Cloud Run service.

E. Use Cloud Run breakglass to deploy an image that meets the Binary Authorization policy by default.

Correct Answer: AB

QUESTION 4

An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well- established directory service is used to manage user identities and lifecycle management. This directory service must continue for the organization to use as the "source of truth" directory for identities.

Which solution meets the organization\\'s requirements?

A. Google Cloud Directory Sync (GCDS)

B. Cloud Identity

C. Security Assertion Markup Language (SAML)

D. Pub/Sub

Correct Answer: A

With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn\\'t migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server. https://support.google.com/a/answer/106368?hl=en

QUESTION 5

You\\'re developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two

main requirements:

Least-privilege access must be enforced at all times. The DevOps team must be able to access the required resources only during the deployment issue.

How should you grant access while following Google-recommended best practices?

A. Assign the Project Viewer Identity and Access Management (1AM) role to the DevOps team.

B. Create a custom 1AM role with limited list/view permissions, and assign it to the DevOps team.

C. Create a service account, and grant it the Project Owner 1AM role. Give the Service Account User Role on this

service account to the DevOps team.

D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Correct Answer: B