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.pass2lead.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

Your organization is moving virtual machines (VMs) to Google Cloud. You must ensure that operating system images that are used across your projects are trusted and meet your security requirements. What should you do?

A. Implement an organization policy to enforce that boot disks can only be created from images that come from the trusted image project.

B. Create a Cloud Function that is automatically triggered when a new virtual machine is created from the trusted image repository Verify that the image is not deprecated.

C. Implement an organization policy constraint that enables the Shielded VM service on all projects to enforce the trusted image repository usage.

D. Automate a security scanner that verifies that no common vulnerabilities and exposures (CVEs) are present in your trusted image repository.

Correct Answer: A

QUESTION 2

Your organization is using GitHub Actions as a continuous integration and delivery (CI/CD) platform. You must enable access to Google Cloud resources from the CI/CD pipelines in the most secure way. What should you do?

A. Create a service account key and add it to the GitHub pipeline configuration file.

B. Create a service account key and add it to the GitHub repository content.

C. Configure a Google Kubernetes Engine cluster that uses Workload Identity to supply credentials to GitHub.

D. Configure workload identity federation to use GitHub as an identity pool provider.

Correct Answer: D

QUESTION 3

Your company has been creating users manually in Cloud Identity to provide access to Google Cloud resources. Due to continued growth of the environment, you want to authorize the Google Cloud Directory Sync (GCDS) instance and

integrate it with your on-premises LDAP server to onboard hundreds of users.

You are required to:

Replicate user and group lifecycle changes from the on-premises LDAP server in Cloud Identity.

Disable any manually created users in Cloud Identity.

You have already configured the LDAP search attributes to include the users and security groups in scope for Google Cloud. What should you do next to complete this solution?

A. 1. Configure the option to suspend domain users not found in LDAP.

2. Set up a recurring GCDS task.

B. 1. Configure the option to delete domain users not found in LDAP.

2. Run GCDS after user and group lifecycle changes.

C. 1. Configure the LDAP search attributes to exclude manually created Cloud Identity users not found in LDAP.

2. Set up a recurring GCDS task.

D. 1. Configure the LDAP search attributes to exclude manually created Cloud identity users not found in LDAP.

2. Run GCDS after user and group lifecycle changes.

Correct Answer: A

To achieve the requirement "Disable any manually created users in Cloud Identity", configure GCDS to suspend rather than delete accounts if user accounts are not found in the LDAP directory in GCDS. Ref: https://support.google.com/a/answer/7177267

QUESTION 4

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer\\'s internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP\\'s native SYN flood protection.

Which product should be used to meet these requirements?

A. Cloud Armor

B. VPC Firewall Rules

C. Cloud Identity and Access Management

D. Cloud CDN

Correct Answer: A

Reference: https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors- new-waf-capabilities

---

QUESTION 5

A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location. Which solution will restrict access to the in-progress sites?

A. Upload an .htaccess file containing the customer and employee user accounts to App Engine.

B. Create an App Engine firewall rule that allows access from the customer and employee networks and denies all other traffic.

C. Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.

D. Use Cloud VPN to create a VPN connection between the relevant on-premises networks and the company\\'s GCP Virtual Private Cloud (VPC) network.

Correct Answer: C

https://cloud.google.com/iap/docs/concepts-overview#when_to_use_iap