Professional-Cloud-Security-Engineer Valid Exam Camp - Google Realistic Google Cloud Certified - Professional Cloud Security Engineer Exam Exam Actual Questions

2026 Latest ActualCollection Professional-Cloud-Security-Engineer PDF Dumps and Professional-Cloud-Security-Engineer Exam Engine Free Share: https://drive.google.com/open?id=1N7WbB7K0fDVkZAldC6sxK1H0h9J2uptt

We keep a close watch at the most advanced social views about the knowledge of the test Google certification. Our experts will renovate the test bank with the latest Professional-Cloud-Security-Engineer study materials and compile the latest knowledge and information into the questions and answers. In the answers, our experts will provide the authorized verification and detailed demonstration so as to let the learners master the latest information timely and follow the trend of the times. All we do is to integrate the most advanced views into our Professional-Cloud-Security-Engineer Study Materials.

Configure Network Security

- **Private Connectivity Establishment:** The consideration for this topic includes enabling private connectivity between Google APIs and VPC as well as private RFC 1918 connectivity between Google Cloud Projects & VPC networks and between VPC network & data centers.
- **Network Security Design:** The test takers will be required to demonstrate an understanding of security properties of VPC networks, shared VPC, firewall rules, and VPC peering. This objective also measures their skills in using DNSSEC, security policy for app-to-app, and network isolation & data encapsulation for N-tier application design;
- **Network Segmentation Configuration:** This part evaluates one's competence in network perimeter controls, and load balancing, including global, SSL proxy, network, TCP load balancer, and HTTP(S);

>> Professional-Cloud-Security-Engineer Valid Exam Camp <<

Professional-Cloud-Security-Engineer Exam Torrent - Google Cloud Certified - Professional Cloud Security Engineer Exam Prep Torrent & Professional-Cloud-Security-Engineer Test Guide

These Google Professional-Cloud-Security-Engineer questions and Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer practice test software that will aid in your preparation. All of these Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer formats are developed by experts. And assist you in passing the Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer Exam on the first try. Professional-Cloud-Security-Engineer practice exam software containing Google Professional-Cloud-Security-Engineer practice tests for your practice and preparation.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q140-Q145):

NEW QUESTION # 140

Your company's users access data in a BigQuery table. You want to ensure they can only access the data during working hours. What should you do?

- A. Assign a BigQuery Data Viewer role along with an 1AM condition that limits the access to specified working hours.
- B. Assign a BigQuery Data Viewer role to a service account that adds and removes the users daily during the specified working hours
- C. Configure Cloud Scheduler so that it triggers a Cloud Functions instance that modifies the organizational policy constraints for BigQuery during the specified working hours.
- D. Run a gsuttl script that assigns a BigQuery Data Viewer role, and remove it only during the specified working hours.

Answer: A

Explanation:
o ensure that users can only access the data in a BigQuery table during working hours, you can assign the BigQuery Data Viewer role with an IAM condition that specifies the allowed access times. This method leverages IAM Conditions, which allow you to define and enforce time-based access policies. Here's how to do it:
Identify the BigQuery Table: Determine which BigQuery table(s) require restricted access.
Create an IAM Policy with Conditions: Define an IAM policy that includes a condition for time-based access.
You can do this using the Google Cloud Console, gcloud command-line tool, or directly editing the IAM policy JSON.
Specify Working Hours: In the IAM condition, specify the time frame during which access is allowed. For example, you can set access to be allowed from 9 AM to 5 PM on weekdays.
Assign the Role with Conditions: Apply the policy to the users or groups who need access. Ensure that the condition is correctly attached to the BigQuery Data Viewer role.
Example using gcloud:
gcloud projects add-iam-policy-binding [PROJECT_ID] \
--member=user:[USER_EMAIL] \
--role=roles/bigquery.dataViewer \
--condition=expression="(request.time.getFullYear() == 2024) && (request.time.getDayOfWeek() in [1, 2, 3,
4, 5]) && (request.time.getHours() >= 9) && (request.time.getHours() < 17)",title="Working hours condition",description="Access limited to working hours" References Google Cloud IAM Conditions Google Cloud BigQuery IAM Roles

NEW QUESTION # 141
You are managing data in your organization's Cloud Storage buckets and are required to retain objects. To reduce storage costs, you must automatically downgrade the storage class of objects older than 365 days to Coldline storage. What should you do?

- A. Define a lifecycle policy JSON with an action on SetStorageClass to COLDLINE with an age condition of 365 and matchStorageClass STANDARD.
- B. Set up a CloudRun Job with Cloud Scheduler to execute a script that searches for and removes flies older than 365 days from your Cloud Storage.
- C. Use Cloud Asset Inventory to generate a report of the configuration of all storage buckets.
  Examine the Lifecycle management policy settings and ensure that they are set correctly.
- D. Enable the Autoclass feature to manage all aspects of bucket storage classes.

Answer: A

Explanation:
Create a lifecycle policy JSON:
Specify an action (SetStorageClass) to move objects to COLDLINE storage.
Include a condition (age) to apply the policy to objects older than 365 days.
Use the matchStorageClass parameter to apply the policy only to objects currently in STANDARD storage, ensuring that objects already in lower-cost classes (e.g., COLDLINE or ARCHIVE) are not unnecessarily moved.

NEW QUESTION # 142
You are responsible for managing your company's identities in Google Cloud. Your company enforces 2-Step Verification (2SV) for all users. You need to reset a user's access, but the user lost their second factor for
2SV. You want to minimize risk. What should you do?

- A. On the Google Admin console, select the appropriate user account, and temporarily disable 2SV for this account Ask the user to update their second factor, and then re-enable 2SV for this account.

- B. On the Google Admin console, select the appropriate user account, and generate a backup code to allow the user to sign in. Ask the user to update their second factor.
- C. On the Google Admin console, temporarily disable the 2SV requirements for all users. Ask the user to log in and add their new second factor to their account. Re-enable the 2SV requirement for all users.
- D. On the Google Admin console, use a super administrator account to reset the user account's credentials.Ask the user to update their credentials after their first login.

Answer: B

Explanation:
If a user loses their second factor for 2-Step Verification (2SV), you can help them regain access with minimal risk by generating a backup code.
* Generate a Backup Code (A):
* In the Google Admin console, navigate to the user's account settings.
* Generate a backup code for the user. This code allows them to sign in despite not having access to their usual second factor.
* Instruct the user to log in using the backup code and then update their second factor in their account settings.
This method ensures that only the affected user's access is temporarily adjusted, minimizing risk while maintaining overall security policies.
References
* Google Admin console 2-Step Verification documentation

NEW QUESTION # 143
Your organization is adopting Google Cloud and wants to ensure sensitive resources are only accessible from devices within the internal on-premises corporate network. You must configure Access Context Manager to enforce this requirement. These considerations apply:
- The internal network uses IP ranges 10.100.0.0/16 and 192.168.0.0/16.
- Some employees work remotely but connect securely through a company-managed virtual private network (VPN). The VPN dynamically allocates IP addresses from the pool 172.16.0.0/20.
- Access should be restricted to a specific Google Cloud project that is contained within an existing service perimeter.
What should you do?

- A. Create an access level titled "Corporate Access." Add a condition with the IP Subnetworks attribute, including the ranges: 10.100.0.0/16, 192.168.0.0/16, 172.16.0.0/20. Assign this access level to a service perimeter encompassing the sensitive project.
- B. Create an access level named "Authorized Devices." Utilize the Device Policy attribute to require corporate-managed devices. Apply the access level to the Google Cloud project and instruct all employees to enroll their devices in the organization's management system.
- C. Create a new IAM role called "InternalAccess. Add the IP ranges 10.100.0.0/16, 192.16.0.0/16, and 172.16.0.0/20 to the role as an IAM condition. Assign this role to IAM groups corresponding to on-premises and VPN users. Grant this role the necessary permissions on the resource within this sensitive Google Cloud project.
- D. Create an access level titled "Internal Network Only." Add a condition with these attributes:
  - IP Subnetworks: 10.100.0.0/16, 192.168.0.0/16
  - Device Policy: Require OS as Windows or macOS. Apply this access level to the sensitive Google Cloud project.

Answer: A

Explanation:
https://cloud.google.com/access-context-manager/docs/overview#ip-address

NEW QUESTION # 144
Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.
Which logging export strategy should you use to meet the requirements?

- A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project.
  2. Subscribe SIEM to the topic.

- B. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.
  2. Subscribe SIEM to the topic.
- C. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project.
  2. Process Cloud Storage objects in SIEM.
- D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.
  2. Process Cloud Storage objects in SIEM.

Answer: C

NEW QUESTION # 145
.....