

Overcome Exam Challenges with Google Professional-Cloud-Security-Engineer Exam Questions

Google Professional Cloud Security Engineer Practice Questions

Google Cloud Certified - Professional Cloud Security Engineer

Order our Professional Cloud Security Engineer Practice Questions Today and Get Ready to Pass with Flying Colors!



Professional Cloud Security Engineer Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

<https://www.questionstube.com/exam/professional-cloud-security-engineer/>

At QuestionsTube, you can read Professional Cloud Security Engineer free demo questions in pdf file, so you can check the questions and answers before deciding to download the Google Professional Cloud Security Engineer practice questions. These free demo questions are parts of the Professional Cloud

DOWNLOAD the newest NewPassLeader Professional-Cloud-Security-Engineer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13pNZ89fi88FywagtHm8_VxfNP3AIK9-v

Our company is a professional certificate test materials provider, and we have rich experiences in providing exam materials. Professional-Cloud-Security-Engineer exam materials are reliable, and we can help you pass the exam just one time. Professional-Cloud-Security-Engineer exam dumps are also known as high pass rate, and the pass rate reaches 98.95%. We are pass guaranteed and money back guaranteed in case you fail to pass the exam. Moreover, we have free demo for Professional-Cloud-Security-Engineer Exam Materials for you to have a general understanding of the product.

The Professional-Cloud-Security-Engineer certification is recognized as a benchmark for cloud security expertise, and it validates an individual's ability to secure GCP environments against potential threats and attacks. Google Cloud Certified - Professional Cloud Security Engineer Exam certification is also proof of an individual's proficiency in implementing security controls and techniques on GCP services and infrastructure. Google Cloud Certified - Professional Cloud Security Engineer Exam certification can help professionals differentiate themselves in the market, and it can lead to career growth opportunities and career advancement within organizations that use GCP.

Google Professional-Cloud-Security-Engineer Exam is a comprehensive certification test that assesses a candidate's knowledge and skills in securing Google Cloud Platform (GCP) systems and infrastructure. As a Google Cloud Certified - Professional Cloud Security Engineer, an individual can authenticate their expertise in designing, implementing, and managing cloud security solutions for businesses and organizations.

>> 100% Professional-Cloud-Security-Engineer Exam Coverage <<

Pass Guaranteed 2025 Professional-Cloud-Security-Engineer: Newest 100% Google Cloud Certified - Professional Cloud Security Engineer Exam Exam Coverage

You can first download NewPassLeader's free exercises and answers about Google certification Professional-Cloud-Security-Engineer exam as a try, then you will feel that NewPassLeader give you a reassurance for passing the exam. If you choose NewPassLeader to provide you with the pertinence training, you can easily pass the Google Certification Professional-Cloud-Security-Engineer Exam.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q99-Q104):

NEW QUESTION # 99

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

- A. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.
- B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.
- **C. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.**
- D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.

Answer: C

Explanation:

Reference:

Envelope Encryption: <https://cloud.google.com/kms/docs/envelope-encryption> Here are best practices for managing DEKs:

-Generate DEKs locally.

-When stored, always ensure DEKs are encrypted at rest.

- For easy access, store the DEK near the data that it encrypts.

The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.

Here are best practices for managing KEKs:

-Store KEKs centrally. (KMS)

-Set the granularity of the DEKs they encrypt based on their use case. For example, consider a workload that requires multiple DEKs to encrypt the workload's data chunks. You could use a single KEK to wrap all DEKs that are responsible for that workload's encryption.

-Rotate keys regularly, and also after a suspected incident.

NEW QUESTION # 100

You have noticed an increased number of phishing attacks across your enterprise user accounts.

You want to implement the Google 2-Step Verification (2SV) option that uses a cryptographic signature to authenticate a user and verify the URL of the login page. Which Google 2SV option should you use?

- A. Google Authenticator app

- Answer: B**

Security keys use public key cryptography to verify a user's identity and URL of the login page ensuring attackers can't access your account even if you are tricked into providing your username and password.

- A. Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems Provide the raw CSEK as part of the API call.
- B. Create a Cloud Key Management Service (KMS) key with imported key material Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.
- C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.
- D. Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM) Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.

- A. Encrypted emails
- B. A strict password policy
- C. Captcha on login pages
- **D. Multifactor Authentication**

- A. BigQuery using a data pipeline job with continuous updates via Cloud VPN
- B. Cloud Datastore using regularly scheduled batch upload jobs via Cloud VPN
- C. Compute Engines Virtual Machines using Persistent Disk via Cloud Interconnect
- D. Cloud Storage using a scheduled task and gsutil via Cloud Interconnect

[illegible]

BONUS!!! Download part of NewPassLeader Professional-Cloud-Security-Engineer dumps for free: https://drive.google.com/open?id=13pNZ89ff88FywagtHm8_VxfNP3AIK9-v