

Professional-Cloud-Security-Engineer Dumps | Professional-Cloud-Security-Engineer Valid Dumps Book



BONUS!!! Download part of Itcertking Professional-Cloud-Security-Engineer dumps for free: <https://drive.google.com/open?id=1Iz64ZkeuT-p0qjEDlbcQrXk1xN6T6C0k>

For candidates who are going to buy Professional-Cloud-Security-Engineer training materials online, you may pay more attention to the money safety. We apply the international recognition third party for the payment, so your account and money safety can be guaranteed if you choose us. In addition, we offer you free demo for you to have a try before buying Professional-Cloud-Security-Engineer Exam Dumps, so that you can have a deeper understanding of what you are going to buy. Professional-Cloud-Security-Engineer exam braindumps contain both questions and answers, and it's convenient for you to check the answers after practicing. We have the online and offline service, and if you have any questions, you can consult us.

Google Professional-Cloud-Security-Engineer Exam is a challenging exam that requires a significant amount of preparation and study. Candidates should have a strong understanding of cloud-based infrastructure and security best practices. They should also have experience designing and implementing security solutions in a cloud-based environment. Candidates who pass the exam will receive a Google Cloud Certified - Professional Cloud Security Engineer certification, which is recognized by organizations around the world. Google Cloud Certified - Professional Cloud Security Engineer Exam certification demonstrates that the candidate has the necessary skills and knowledge to secure cloud-based infrastructure on the Google Cloud Platform.

>> Professional-Cloud-Security-Engineer Dumps <<

Professional-Cloud-Security-Engineer Dumps - Google Professional-Cloud-Security-Engineer Valid Dumps Book: Google Cloud Certified - Professional Cloud Security Engineer Exam Exam Pass Once Try

Many candidates felt worried about their exam for complex content and too extensive subjects to choose and understand. Our Professional-Cloud-Security-Engineer exam materials successfully solve this problem for them, with the simplified language and key to point subjects, you are easy to understand and grasp all the information that in our Professional-Cloud-Security-Engineer training guide. For Our professionals compiled them with the purpose that help all of the customer to pass their Professional-Cloud-Security-Engineer exam.

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q137-Q142):

NEW QUESTION # 137

Your privacy team uses crypto-shredding (deleting encryption keys) as a strategy to delete personally identifiable information (PII). You need to implement this practice on Google Cloud while still utilizing the majority of the platform's services and minimizing operational overhead. What should you do?

- A. Use Google default encryption to delete specific encryption keys.
- B. Use Cloud External Key Manager to delete specific encryption keys.
- C. Use client-side encryption before sending data to Google Cloud, and delete encryption keys on-premises
- D. Use customer-managed encryption keys to delete specific encryption keys.

Answer: D

Explanation:

Explanation

<https://cloud.google.com/sql/docs/mysql/cmek>

"You might have situations where you want to permanently destroy data encrypted with CMEK. To do this, you destroy the customer-managed encryption key version. You can't destroy the keyring or key, but you can destroy key versions of the key."

NEW QUESTION # 138

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. Cloud HSM keys
- B. Titan Security Keys
- C. Google Authenticator app
- D. Google prompt

Answer: B

Explanation:

Explanation

<https://cloud.google.com/titan-security-key>

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.

NEW QUESTION # 139

You need to connect your organization's on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?

- A. 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.
2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.
- B. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.
2. Configure private access for both VPC subnets.
- C. 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.
2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.
- D. 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.
2. Configure private access using the restricted googleapis.com domains in on-premises DNS configurations.

Answer: A

Explanation:

Explanation

restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC Service Controls. VPC Service Controls are enforced for these services <https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid>

NEW QUESTION # 140

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. Cloud Identity
- B. Identity-Aware Proxy
- C. SSO SAML as a third-party IdP
- D. Identity Platform
- E. OpenID Connect

Answer: C,E

Explanation:

Explanation

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>

NEW QUESTION # 141

You are setting up Cloud Identity for your company's Google Cloud organization. User accounts will be provisioned from Microsoft Entra ID through Directory Sync, and there will be single sign-on through Entra ID. You need to secure the super administrator accounts for the organization. Your solution must follow the principle of least privilege and implement strong authentication. What should you do?

- A. Create dedicated accounts for super administrators. Ensure that 2-step verification is enforced for the super administrator accounts in Entra ID
- B. Create accounts that combine the organization administrator and the super administrator privileges. Ensure that 2-step verification is enforced for the super administrator accounts in Entra ID
- C. Create accounts that combine the organization administrators and the super administrator privileges. Enforce Google 2-step verification for the super administrator accounts
- D. Create dedicated accounts for super administrators. Enforce Google 2-step verification for the super administrator accounts

Answer: D

Explanation:

The problem focuses on securing "super administrator accounts for the organization" when Cloud Identity is synced with Microsoft Entra ID and uses Entra ID for SSO. The key requirements are the principle of least privilege and strong authentication. Principle of Least Privilege & Dedicated Accounts: Google's best practices strongly recommend creating dedicated, non-federated accounts for super administrators that are distinct from regular user accounts. These accounts should only be used for super administrator tasks and not for daily activities. This segregation ensures that the highest privilege accounts are isolated and adhere to the principle of least privilege by not having combined responsibilities. Extract Reference: "Designate Organization Administrators. We recommend keeping your super admin account separate from your Organization Administrator group" and "Give super admins a separate account that requires a separate login. For example, user alice@example.com could have a super admin account alice-admin@example.com" and "Use the super admin account only when needed. Delegate administrator tasks to user accounts with limited admin roles. Use the least privilege approach" (Google Cloud Documentation: "Super administrator account best practices | Resource Manager Documentation" - <https://cloud.google.com/resource-manager/docs/super-admin-best-practices>). Strong Authentication (Google 2-Step Verification): Even when using a third-party identity provider like Microsoft Entra ID for most users, Google recommends enforcing Google's own 2-Step Verification for the critical super administrator accounts. This provides a "break-glass" mechanism that is independent of the external IdP. If the Entra ID integration were to fail or become compromised, the Google-managed super administrator accounts, protected by Google's own 2SV, would still be accessible for emergency recovery. Extract Reference: "Even when using the legacy SSO profile, super admins can't sign in with SSO in these cases: Admin console. When super administrators try to sign in to an SSO-enabled domain via admingle.google.com, they must enter their full Google administrator account email address and associated Google password (not their SSO username and password), and click Sign in to directly access the Admin console".

Google doesn't redirect them to the SSO sign-in page" (Google Cloud Identity Help: "Super administrator SSO" - <https://support.google.com/cloudidentity/answer/6341409>) - This highlights that super admin accounts can bypass SSO for direct Admin console access, making Google's 2SV crucial Extract Reference: "It's especially important for super admins to use 2SV because their accounts control access to all business and employee data in the organization Protect your business with 2-Step Verification Use security keys for 2-Step Verification" (Cloud Identity Help: "Security best practices for administrator accounts" - <https://support.google.com/cloudidentity/answer/9011373>)

NEW QUESTION # 142

Itcertking's Google Professional-Cloud-Security-Engineer exam training materials are the necessities of each of candidates who participating in the IT certification. With this training material, you can do a full exam preparation. So that you will have the confidence to win the exam. Itcertking's Google Professional-Cloud-Security-Engineer Exam Training materials are highly targeted. Not every training materials on the Internet have such high quality. Only Itcertking could be so perfect.

Professional-Cloud-Security-Engineer Valid Dumps Book: https://www.itcertking.com/Professional-Cloud-Security-Engineer_exam.html

BTW, DOWNLOAD part of Itcertking Professional-Cloud-Security-Engineer dumps from Cloud Storage:
<https://drive.google.com/open?id=1Iz64ZkeuT-p0qjEDlbcQrXk1xN6T6C0k>