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.passapply.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 are in charge of creating a new Google Cloud organization for your company. Which two actions should you take when creating the super administrator accounts? (Choose two.)

A. Create an access level in the Google Admin console to prevent super admin from logging in to Google Cloud.

B. Disable any Identity and Access Management (1AM) roles for super admin at the organization level in the Google Cloud Console.

C. Use a physical token to secure the super admin credentials with multi-factor authentication (MFA).

D. Use a private connection to create the super admin accounts to avoid sending your credentials over the Internet.

E. Provide non-privileged identities to the super admin users for their day-to-day activities.

Correct Answer: CE

https://cloud.google.com/resource-manager/docs/super-admin-best-practices#discourage_super_admin_account_usage

1.

Use a security key or other physical authentication device to enforce two-step verification

2.

Give super admins a separate account that requires a separate login

QUESTION 2

A company is using Google Kubernetes Engine (GKE) with container images of a mission-critical application. The company wants to scan the images for known security issues and securely share the report with the security team without exposing them outside Google Cloud.

What should you do?

A. 1. Enable Container Threat Detection in the Security Command Center Premium tier.

2.

Upgrade all clusters that are not on a supported version of GKE to the latest possible GKE version.

3.

View and share the results from the Security Command Center.

B. 1. Use an open source tool in Cloud Build to scan the images.

2.

Upload reports to publicly accessible buckets in Cloud Storage by using gsutil.

3.

Share the scan report link with your security department.

C. 1. Enable vulnerability scanning in the Artifact Registry settings.

2.

Use Cloud Build to build the images.

3.

Push the images to the Artifact Registry for automatic scanning.

4.

View the reports in the Artifact Registry.

D. 1. Get a GitHub subscription.

2.

Build the images in Cloud Build and store them in GitHub for automatic scanning.

3.

Download the report from GitHub and share with the Security Team.

Correct Answer: C

QUESTION 3

Your organization wants full control of the keys used to encrypt data at rest in their Google Cloud environments. Keys must be generated and stored outside of Google and integrate with many Google Services including BigQuery. What should you do?

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 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.

C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

D. 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.

Correct Answer: C

The correct answer is C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

Cloud EKM allows you to use encryption keys that are stored and managed in a third-party key management system deployed outside of Google\\'s infrastructure. This gives your organization full control over the keys used to encrypt data

at rest in Google Cloud environments, including BigQuery.

QUESTION 4

You are designing a new governance model for your organization\\'s secrets that are stored in Secret Manager. Currently, secrets for Production and Non-Production applications are stored and accessed using service accounts. Your proposed solution must:

Provide granular access to secrets

Give you control over the rotation schedules for the encryption keys that wrap your secrets

Maintain environment separation

Provide ease of management

Which approach should you take?

A. 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

2.

Enforce access control to secrets using project-level identity and Access Management (IAM) bindings.

3.

Use customer-managed encryption keys to encrypt secrets.

B. 1. Use a single Google Cloud project to store both Production and Non-Production secrets.

2.

Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings.

3.

Use Google-managed encryption keys to encrypt secrets.

C. 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

2.

Enforce access control to secrets using secret-level Identity and Access Management (IAM) bindings.

3.

Use Google-managed encryption keys to encrypt secrets.

D. 1. Use a single Google Cloud project to store both Production and Non-Production secrets.

2.

Enforce access control to secrets using project-level Identity and Access Management (IAM) bindings.

3.

Use customer-managed encryption keys to encrypt secrets.

Correct Answer: A

Provide granular access to secrets: 2.Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. Give you control over the rotation schedules for the encryption keys that wrap your secrets: 3. Use customer-managed encryption keys to encrypt secrets. Maintain environment separation: 1. Use separate Google Cloud projects to store Production and Non-Production secrets.

QUESTION 5

Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet.

What should your team grant to Engineering Group A to meet this requirement?

A. Compute Network User Role at the host project level.

B. Compute Network User Role at the subnet level.

C. Compute Shared VPC Admin Role at the host project level.

D. Compute Shared VPC Admin Role at the service project level.

Correct Answer: B

https://cloud.google.com/vpc/docs/shared-vpc#svc_proj_admins