vmexam.com
#1 Cloud and VM Certification Guide

Google GCP-PCSE

Google Professional Cloud Security Engineer Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

GCP-PCSE

Google Cloud Platform - Professional Cloud Security Engineer (GCP-PCSE)

50 Questions Exam – 70% Cut Score – Duration of 120 minutes

Table of Contents:

Discover More about the GCP-PCSE Certification

Are you interested in passing the Google GCP-PCSE exam? First discover, who benefits from the GCP-PCSE certification. The GCP-PCSE is suitable for a candidate if he wants to learn about Cloud. Passing the GCP-PCSE exam earns you the Google Cloud Platform - Professional Cloud Security Engineer (GCP-PCSE) title.

While preparing for the GCP-PCSE exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The GCP-PCSE PDF contains some of the most valuable preparation tips and the details and instant access to useful **GCP-PCSE study materials just at one click**.

Google GCP-PCSE Professional Cloud Security Engineer Certification Details:

Exam Name	Google Professional Cloud Security Engineer
Exam Code	GCP-PCSE
Exam Price	$200 USD
Duration	120 minutes
Number of Questions	50
Passing Score	Pass / Fail (Approx 70%)
Recommended Training / Books	**Google Cloud training** **Google Cloud documentation** **Google Cloud solutions**
Schedule Exam	**PEARSON VUE**
Sample Questions	**Google GCP-PCSE Sample Questions**
Recommended Practice	**Google Cloud Platform - Professional Cloud Security Engineer (GCP-PCSE) Practice Test**

GCP-PCSE Syllabus:

Section	**Objectives**
Configuring access within a cloud solution environment	
Configuring Cloud Identity. Considerations include:	- Managing Cloud Identity - Configuring Google Cloud Directory Sync - Managing super administrator account - Automating user lifecycle management process - Administering user accounts and groups programmatically

Section	Objectives
Managing service accounts. Considerations include:	- Protecting and auditing service accounts and keys - Automating the rotation of user-managed service account keys - Identifying scenarios requiring service accounts - Creating, authorizing, and securing service accounts - Securely managing API access management - Managing and creating short-lived credentials
Managing authentication. Considerations include:	- Creating a password policy for user accounts - Establishing Security Assertion Markup Language (SAML) - Configuring and enforcing two-factor authentication
Managing and implementing authorization controls. Considerations include:	- Managing privileged roles and separation of duties - Managing IAM permissions with basic, predefined, and custom roles - Granting permissions to different types of identities - Understanding difference between Cloud Storage IAM and ACLs - Designing identity roles at the organization, folder, project, and resource level - Configuring Access Context Manager
Defining resource hierarchy. Considerations include:	- Creating and managing organizations - Designing resource policies for organizations, folders, projects, and resources - Managing organization constraints - Using resource hierarchy for access control and permissions inheritance - Designing and managing trust and security boundaries within Google Cloud projects
Configuring network security	
Designing network security. Considerations include:	- Configuring network perimeter controls (firewall rules; Identity-Aware Proxy (IAP)) - Configuring load balancing (global, network, HTTP(S), SSL proxy, and TCP proxy load balancers) - Identifying Domain Name System Security Extensions (DNSSEC) - Identifying differences between private versus public addressing - Configuring web application firewall (Google Cloud Armor) - Configuring Cloud DNS
Configuring network segmentation.	- Configuring security properties of a VPC network, VPC peering, Shared VPC, and firewall rules - Configuring network isolation and data encapsulation for N

Section	Objectives
Considerations include:	tier application design - Configuring app-to-app security policy
Establishing private connectivity. Considerations include:	- Designing and configuring private RFC1918 connectivity between VPC networks and Google Cloud projects (Shared VPC, VPC peering) - Designing and configuring private RFC1918 connectivity between data centers and VPC network (IPSEC and Cloud Interconnect). - Establishing private connectivity between VPC and Google APIs (Private Google Access, Private Google Access for on-premises hosts, Private Service Connect) - Configuring Cloud NAT
Ensuring data protection	
Protecting sensitive data. Considerations include:	- Inspecting and redacting personally identifiable information (PII) - Configuring pseudonymization - Configuring format-preserving substitution - Restricting access to BigQuery datasets - Configuring VPC Service Controls - Securing secrets with Secret Manager - Protecting and managing compute instance metadata
Managing encryption at rest. Considerations include:	- Understanding use cases for Google default encryption, customer-managed encryption keys (CMEK), customer-supplied encryption keys (CSEK), Cloud External Key Manager (EKM), and Cloud HSM - Creating and managing encryption keys for CMEK, CSEK, and EKM - Applying Google's encryption approach to use cases - Configuring object lifecycle policies for Cloud Storage - Enabling confidential computing
Managing operations in a cloud solution environment	
Building and deploying secure infrastructure and applications. Considerations include:	- Automating security scanning for Common Vulnerabilities and Exposures (CVEs) through a CI/CD pipeline - Automating virtual machine image creation, hardening, and maintenance - Automating container image creation, verification, hardening, maintenance, and patch management
Configuring logging, monitoring, and detection.	- Configuring and analyzing network logs (firewall rule logs, VPC flow logs, packet mirroring) - Designing an effective logging strategy - Logging, monitoring, responding to, and remediating security incidents

Section	Objectives
Considerations include:	- Exporting logs to external security systems - Configuring and analyzing Google Cloud audit logs and data access logs - Configuring log exports (log sinks, aggregated sinks, logs router) - Configuring and monitoring Security Command Center (Security Health Analytics, Event Threat Detection, Container Threat Detection, Web Security Scanner)
Ensuring compliance	
Determining regulatory requirements for the cloud. Considerations include:	- Determining concerns relative to compute, data, and network - Evaluating security shared responsibility model - Configuring security controls within cloud environments - Limiting compute and data for regulatory compliance - Determining the Google Cloud environment in scope for regulatory compliance

Broaden Your Knowledge with Google GCP-PCSE Sample Questions:

Question: 1

You want to protect the default VPC network from all inbound and outbound internet traffic. What action should you take?

a) Create a Deny All inbound internet firewall rule.
b) Create a Deny All outbound internet firewall rule.
c) Create a new subnet in the VPC network with private Google access enabled.
d) Create instances without external IP addresses only.

Answer: b

Question: 2

Which encryption algorithm is used with Default Encryption in Cloud Storage?

a) AES-256
b) SHA512
c) MD5
d) 3DES

Answer: a

Question: 3

An organization is working on their GDPR compliance strategy. It wants to ensure that controls are in place to ensure that customer PII is stored in Cloud Storage buckets without third-party exposure.

Which Google Cloud solution should the organization use to verify that PII is stored in the correct place without exposing PII internally?

a) Cloud Storage Bucket Lock
b) VPC Service Controls
c) Cloud Data Loss Prevention API
d) Cloud Security Scanner

Answer: c

Question: 4

A cloud customer has an on-premises key management system and wants to generate, protect, rotate, and audit encryption keys with it.

How can the customer use Cloud Storage with their own encryption keys?

a) Declare usage of default encryption at rest in the audit report on compliance
b) Upload encryption keys to the same Cloud Storage bucket
c) Use Customer Managed Encryption Keys (CMEK)
d) Use Customer-Supplied Encryption Keys (CSEK)

Answer: d

Question: 5

Your company is deploying their applications on Google Kubernetes Engine. You want to follow Google-recommended practices.

What should you do to ensure that the container images used for new deployments contain the latest security patches?

a) Use an update script as part of every container image startup.
b) Use Container Analysis to detect vulnerabilities in images.
c) Use Google-managed base images for all containers.
d) Use exclusively private images in Container Registry.

Answer: c

Question: 6

You are responsible for implementing a payment processing environment that will use Kubernetes and need to apply proper security controls.

What should you do?

a) Implement and enforce two-factor authentication.
b) Activate a firewall to prevent all egress traffic.
c) Establish minimum password length requirements for all systems.
d) Require file integrity monitoring and antivirus scans of pods and nodes.

Answer: d

Question: 7

Your company is storing files on Cloud Storage. To comply with local regulations, you want to ensure that uploaded files cannot be deleted within the first 5 years.

It should not be possible to lower the retention period after it has been set. What should you do?

a) Apply a retention period of 5 years to the bucket, and lock the bucket.
b) Enable Temporary hold and apply a retention period of 5 years to the bucket.
c) Use Cloud IAM to ensure that nobody has an IAM role that has the permissions to delete files from Cloud Storage.
d) Create an object lifecycle rule using the Age condition and the Delete action. Set the Age condition to 5 years.

Answer: a

Question: 8

You have defined subnets in a VPC within Google Cloud Platform. You need multiple projects to create Compute Engine instances with IP addresses from these subnets. What should you do?

a) Configure Cloud VPN between the projects.
b) Set up VPC peering between all related projects.
c) Change the VPC subnets to enable private Google access.
d) Use Shared VPC to share the subnets with the other projects.

Answer: d

Question: 9

A customer wants to grant access to their application running on Compute Engine to write only to a specific Cloud Storage bucket.

How should you grant access?

a) Create a service account for the application, and grant Cloud Storage Object Creator permissions to the project.
b) Create a service account for the application, and grant Cloud Storage Object Creator permissions at the bucket level.
c) Create a user account, authenticate with the application, and grant Google Storage Admin permissions at the bucket level.
d) Create a user account, authenticate with the application, and grant Google Storage Admin permissions at the project level.

Answer: b

Question: 10

A Cloud Development team needs to use service accounts extensively in their local development. You need to provide the team with the keys for these service accounts. You want to follow Google-recommended practices.

What should you do?

a) Implement a daily key rotation process that generates a new key and commits it to the source code repository every day.
b) Implement a daily key rotation process, and provide developers with a Cloud Storage bucket from which they can download the new key every day.
c) Create a Google Group with all developers. Assign the group the IAM role of Service Account User, and have developers generate and download their own keys.
d) Create a Google Group with all developers. Assign the group the IAM role of Service Account Admin, and have developers generate and download their own keys.

Answer: b

Avail the Study Guide to Pass Google GCP-PCSE Professional Cloud Security Engineer Exam:

- Find out about the GCP-PCSE syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **GCP-PCSE syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the

best plan for yourself to cover each part of the syllabus in a hassle-free manner.

- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the GCP-PCSE training. Joining the Google provided training for GCP-PCSE exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **GCP-PCSE sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. GCP-PCSE practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the GCP-PCSE exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.