Google GCP-PCNE

Google Professional Cloud Network Engineer Certification Questions & Answers

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

GCP-PCNE

Google Cloud Platform - Professional Cloud Network Engineer (GCP-PCNE)

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

Table of Contents:

Discover More about the GCP-PCNE Certification

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

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

Google GCP-PCNE Professional Cloud Network Engineer Certification Details:

Exam Name	Google Professional Cloud Network Engineer
Exam Code	GCP-PCNE
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-PCNE Sample Questions**
Recommended Practice	**Google Cloud Platform - Professional Cloud Network Engineer (GCP-PCNE) Practice Test**

GCP-PCNE Syllabus:

Section	Objectives
Designing, planning, and prototyping a Google Cloud network	
Designing an overall network architecture. Considerations include:	- High availability, failover, and disaster recovery strategies - DNS strategy (e.g., on-premises, Cloud DNS) - Security and data exfiltration requirements - Load balancing - Applying quotas per project and per VPC - Hybrid connectivity (e.g., Google private access for hybrid connectivity) - Container networking - IAM roles - SaaS, PaaS, and IaaS services - Microsegmentation for security purposes (e.g., using metadata, tags, service accounts)
Designing Virtual Private Cloud (VPC) instances. Considerations include:	- IP address management and bring your own IP (BYOIP) - Standalone vs. Shared VPC - Multiple vs. single - Regional vs. multi-regional - VPC Network Peering - Firewalls (e.g., service account-based, tag-based) - Custom routes - Using managed services (e.g., Cloud SQL, Memorystore) - Third-party device insertion (NGFW) into VPC using multi-NIC and internal load balancer as a next hop or equal-cost multi-path (ECMP) routes
Designing a hybrid and multi-cloud network. Considerations include:	- Dedicated Interconnect vs. Partner Interconnect - Multi-cloud connectivity - Direct Peering - IPsec VPN - Failover and disaster recovery strategy - Regional vs. global VPC routing mode - Accessing multiple VPCs from on-premises locations (e.g., Shared VPC, multi-VPC peering topologies) - Bandwidth and constraints provided by hybrid connectivity solutions - Accessing Google Services/APIs privately from on-premises locations - IP address management across on-premises locations

Section	Objectives
	and cloud - DNS peering and forwarding
Designing an IP addressing plan for Google Kubernetes Engine. Considerations include:	- Public and private cluster nodes - Control plane public vs. private endpoints - Subnets and alias IPs - RFC 1918, non-RFC 1918, and privately used public IP (PUPI) address options
Implementing Virtual Private Cloud (VPC) instances	
Configuring VPCs. Considerations include:	- Google Cloud VPC resources (e.g., networks, subnets, firewall rules) - VPC Network Peering - Creating a Shared VPC network and sharing subnets with other projects - Configuring API access to Google services (e.g., Private Google Access, public interfaces) - Expanding VPC subnet ranges after creation
Configuring routing. Considerations include:	- Static vs. dynamic routing - Global vs. regional dynamic routing - Routing policies using tags and priority - Internal load balancer as a next hop - Custom route import/export over VPC Network Peering
Configuring and maintaining Google Kubernetes Engine clusters. Considerations include:	- VPC-native clusters using alias IPs - Clusters with shared VPC - Creating Kubernetes Network Policies - Private clusters and private control plane endpoints - Adding authorized networks for cluster control plane endpoints
Configuring and managing firewall rules. Considerations include:	- Target network tags and service accounts - Rule priority - Network protocols - Ingress and egress rules - Firewall rule logging - Firewall Insights - Hierarchical firewalls
Implementing VPC Service Controls. Considerations include:	- Creating and configuring access levels and service perimeters - VPC accessible services - Perimeter bridges - Audit logging - Dry run mode

Section	Objectives
Configuring network services	
Configuring load balancing. Considerations include:	- Backend services and network endpoint groups (NEGs) - Firewall rules to allow traffic and health checks to backend services - Health checks for backend services and target instance groups - Configuring backends and backend services with balancing method (e.g., RPS, CPU, Custom), session affinity, and capacity scaling/scaler - TCP and SSL proxy load balancers - Load balancers (e.g., External TCP/UDP Network Load Balancing, Internal TCP/UDP Load Balancing, External HTTP(S) Load Balancing, Internal HTTP(S) Load Balancing) - Protocol forwarding - Accommodating workload increases using autoscaling vs. manual scaling
Configuring Google Cloud Armor policies. Considerations include:	- Security policies - Web application firewall (WAF) rules (e.g., SQL injection, cross-site scripting, remote file inclusion) - Attaching security policies to load balancer backends
Configuring Cloud CDN. Considerations include:	- Enabling and disabling Cloud CDN - Cache keys - Invalidating cached objects - Signed URLs - Custom origins
Configuring and maintaining Cloud DNS. Considerations include:	- Managing zones and records - Migrating to Cloud DNS - DNS Security Extensions (DNSSEC) - Forwarding and DNS server policies - Integrating on-premises DNS with Google Cloud - Split-horizon DNS - DNS peering - Private DNS logging
Configuring Cloud NAT. Considerations include:	- Addressing - Port allocations - Customizing timeouts - Logging and monitoring - Restrictions per organization policy constraints
Configuring network packet inspection. Considerations include:	- Packet Mirroring in single and multi-VPC topologies - Capturing relevant traffic using Packet Mirroring source and traffic filters - Routing and inspecting inter-VPC traffic using multi-NIC

Section	Objectives
	VMs (e.g., next-generation firewall appliances) - Configuring an internal load balancer as a next hop for highly available multi-NIC VM routing
Implementing hybrid interconnectivity	
Configuring Cloud Interconnect. Considerations include:	- Dedicated Interconnect connections and VLAN attachments - Partner Interconnect connections and VLAN attachments
Configuring a site-to-site IPsec VPN. Considerations include:	- High availability VPN (dynamic routing) - Classic VPN (e.g., route-based routing, policy-based routing)
Configuring Cloud Router. Considerations include:	- Border Gateway Protocol (BGP) attributes (e.g., ASN, route priority/MED, link-local addresses) - Custom route advertisements via BGP - Deploying reliable and redundant Cloud Routers
Managing, monitoring, and optimizing network operations	
Logging and monitoring with Google Cloud's operations suite. Considerations include:	- Reviewing logs for networking components (e.g., VPN, Cloud Router, VPC Service Controls) - Monitoring networking components (e.g., VPN, Cloud Interconnect connections and interconnect attachments, Cloud Router, load balancers, Google Cloud Armor, Cloud NAT)
Managing and maintaining security. Considerations include:	- Firewalls (e.g., cloud-based, private) - Diagnosing and resolving IAM issues (e.g., Shared VPC, security/network admin)
Maintaining and troubleshooting connectivity issues. Considerations include:	- Draining and redirecting traffic flows with HTTP(S) Load Balancing - Monitoring ingress and egress traffic using VPC Flow Logs - Monitoring firewall logs and Firewall Insights - Managing and troubleshooting VPNs - Troubleshooting Cloud Router BGP peering issues
Monitoring, maintaining, and troubleshooting latency and traffic flow. Considerations include:	- Testing network throughput and latency - Diagnosing routing issues - Using Network Intelligence Center to visualize topology, test connectivity, and monitor performance

Broaden Your Knowledge with Google GCP-PCNE Sample Questions:

Question: 1

Your application development team is beta-testing a new application over Dedicated Interconnect. This application uses a single TCP socket and requires 7-Gbps bandwidth for optimal performance.

The development team notices that connectivity speed of the application is capped at 3 Gbps over Dedicated Interconnect. You want to resolve this problem.

What should you do?

a) Order a new Interconnect to increase bandwidth.
b) Create a Cloud VPN in addition to the Interconnect, and ECMP traffic over both.
c) Instruct the development team to distribute their application traffic over multiple TCP flow sessions.
d) Instruct the development team to tune their application TCP congestion window, receive window, and all other tcp buffers.

Answer: c

Question: 2

One of the secure web applications in your GCP project is currently only serving users in North America.

All of the application's resources are currently hosted in a single GCP region. The application uses a large catalog of graphical assets from a Cloud Storage bucket.

You are notified that the application now needs to serve global clients without adding any additional GCP regions or Compute Engine instances.

What should you do?

a) Configure Cloud CDN.
b) Configure a TCP Proxy.
c) Configure a Network load balancer.
d) Configure Dynamic Routing for the subnet hosting the application.

Answer: a

Question: 3

You are configuring the backend service for a new Google Cloud HTTPS load balancer. The application requires high availability and multiple subnets and needs to scale automatically.

Which backend configuration should you choose?

a) A Zonal Managed Instance Group
b) A Regional Managed Instance Group
c) An Unmanaged Instance Group
d) A Network Endpoint Group

Answer: b

Question: 4

Your new project currently requires 5 gigabits per second (Gbps) of egress traffic from your Google Cloud environment to your company's private data center, but may scale up to 80 Gbps of traffic in the future.

You do not have any public addresses to use. Your company is looking for the most cost-effective long-term solution.

Which type of connection should you use?

a) Carrier Peering
b) Partner Interconnect
c) Dedicated Interconnect
d) A single Virtual Private Network (VPN) tunnel

Answer: c

Question: 5

You have a Dedicated Interconnect with two 10-Gbps links. You want to create a Stackdriver alerting policy that will notify you if either of the two links goes down. Which alerts should you add to the policy?

a) An alert for when the Circuit Operational Status metric threshold for either circuit falls below 1.
b) An alert for when the Interconnect Operational Status metric threshold for the interconnect falls below 1.
c) An alert for when the Interconnect Network Capacity metric threshold for the interconnect falls below 20.
d) An alert for when the Interconnect Dropped Packets metric threshold for the interconnect goes above 0.

Answer: a

Question: 6

Your manager has asked for a list of all Custom Roles with stage General Availability within Identity Access Management. What should you do?

a) From the GCloud Command line, run "gcloud iam list-testable-permissions".
b) From the GCloud Command line, run "gcloud iam roles list --project vpcuser09project".
c) Open the IAM Console and sort Custom Roles. Gather the required information from the Status Field.
d) Open the IAM Console and sort Custom Roles. Gather the required information from the Permissions Field.

Answer: b

Question: 7

You are using a single Cloud Router to exchange routes between your VPC and on-premises network with Dedicated Interconnect. You want to make sure you can still forward traffic, even if all the Cloud Routers in a region go down.

What should you do?

a) Use static routes as a backup to Cloud Router.
b) Turn on graceful restart on your on-premises router.
c) Turn on global routing in your VPC, and create another Cloud Router in a different region.
d) Create a second Cloud Router in the same region, but with a Border Gateway Protocol (BGP) session to a second on-premises device.

Answer: c

Question: 8

You are designing a new VPC network that will route traffic to networks in your company's private data center. You want to ensure that your VPC can support high availability in the future.

The data center team requires you to use a routing protocol that can dynamically fail over if there is a link failure in the data center. Your management requires your design to use only native cloud services.

Which routing protocol should you use?

a) BGP
b) RIP
c) OSPF
d) Static routing

Answer: a

Question: 9

Your company uses a physical security appliance for intrusion detection in its on-premises data center. Your company wants to collect telemetry data using a VPN that connects the GCP environment with the on-premises data center.

You want to implement a solution that will integrate the GCP environment and transfer telemetry data to the on-premises physical security appliance as quickly and effectively as possible.

What should you do?

a) Set up iptables in all Compute Engine instances in GCP to track connection sessions.
b) Route all traffic in the GCP environment to on-premises for inspection before forwarding back to GCP.
c) Write a script that uses Stackdriver and GCP network logging information to collect and analyze monitoring data for intrusion detection.
d) Deploy a GCP Marketplace virtual security appliance from the same vendor with a multi-nic instance, and grant the security team access to configure the instance as needed.

Answer: d

Question: 10

You created two subnets named Test and Web in the same VPC network. You enabled VPC Flow Logs for the Web subnet.

You are trying to connect instances in the Test subnet to the web servers running in the Web subnet, but all of the connections are failing.

You do not see any entries in the Stackdriver logs. What should you do?

a) Enable VPC Flow Logs for the Test subnet also.
b) Make sure that there is a valid entry in the route table.
c) Add a firewall rule to allow traffic from the Test subnet to the Web subnet.
d) Create a subnet in another VPC, and move the web servers in the new subnet.

Answer: c

Avail the Study Guide to Pass Google GCP-PCNE Professional Cloud Network Engineer Exam:

- Find out about the GCP-PCNE 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-PCNE 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-PCNE training. Joining the Google provided training for GCP-PCNE 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-PCNE sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. GCP-PCNE 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-PCNE 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.

Here Is the Trusted Practice Test for the GCP-PCNE Certification

VMExam.Com is here with all the necessary details regarding the GCP-PCNE exam. We provide authentic practice tests for the GCP-PCNE exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on VMExam.Com for rigorous, unlimited two-month attempts on the **GCP-PCNE practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Google Cloud Platform - Professional Cloud Network Engineer (GCP-PCNE).

Start Online practice of GCP-PCNE Exam by visiting URL
https://www.vmexam.com/google/gcp-pcne-google-professional-cloud-network-engineer