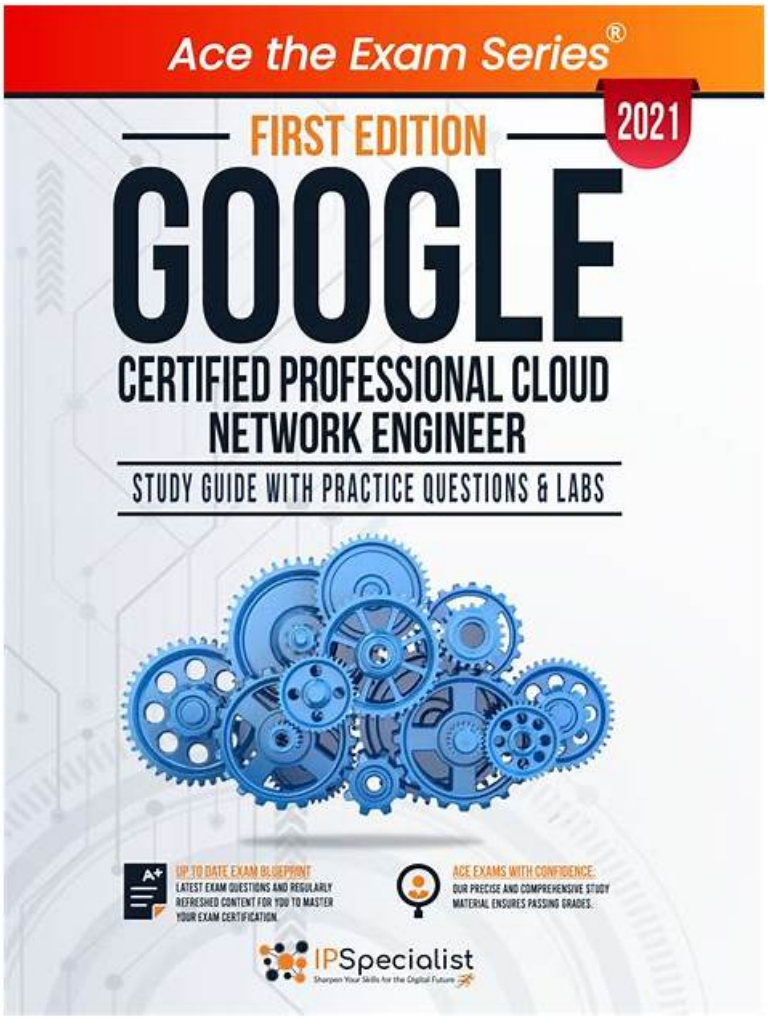
Comprehensive Google Professional-Cloud-Network-Engineer Questions in PDF Format



BONUS!!! Download part of PDFDumps Professional-Cloud-Network-Engineer dumps for free: https://drive.google.com/open?id=1xEAu9AgD8hXL2hF3PW6j2bppMujR8zCR

Our Google Cloud Certified - Professional Cloud Network Engineer (Professional-Cloud-Network-Engineer) PDF file is portable which means customers can carry this real questions document to any place. You just need smartphones, or laptops, to access this Google Cloud Certified - Professional Cloud Network Engineer (Professional-Cloud-Network-Engineer) PDF format. These Google Cloud Certified - Professional Cloud Network Engineer (Professional-Cloud-Network-Engineer) questions PDFs are also printable. So candidates who prefer to study in the old way which is paper study can print Google Cloud Certified - Professional Cloud Network Engineer (Professional-Cloud-Network-Engineer) questions PDF as well.

To prepare for the Google Professional-Cloud-Network-Engineer Certification Exam, candidates should have a solid understanding of networking concepts and protocols, as well as hands-on experience with GCP. Google offers a number of resources to help candidates prepare for the exam, including online courses, practice exams, and study guides.

>> Professional-Cloud-Network-Engineer Upgrade Dumps <<

Actual Professional-Cloud-Network-Engineer Test Prep is Attributive Practice Questions to High-Efficient Learning

Our APP version of Professional-Cloud-Network-Engineer exam questions can support almost any electronic device, from iPod, telephone, to computer and so on. You can use Our Professional-Cloud-Network-Engineer test torrent by your telephone when you

are travelling far from home; I think it will be very convenient for you. You can also choose to use our Professional-Cloud-Network-Engineer Study Materials by your computer when you are at home. You just need to download the online version of our Professional-Cloud-Network-Engineer study materials, which is not limited to any electronic device and support all electronic equipment in anywhere and anytime.

Google Cloud Certified - Professional Cloud Network Engineer Sample Questions (Q212-Q217):

NEW QUESTION # 212
You are implementing a VPC architecture for your organization by using a Network Connectivity Center hub and spoke topology:
* There is one Network Connectivity Center hybrid spoke to receive on-premises routes.
* There is one VPC spoke that needs to be added as a Network Connectivity Center spoke.
Your organization has limited routable IP space fortheir cloud environment (192.168.0.0/20). The Network Connectivity Center spoke VPC is connected to on-premises with a Cloud Interconnect connection in the us- east4 region. The on-premises IP range is 172.16.0.0/16. You need to reach on-premises resources from multiple Google Cloud regions (us-westl, europe-centrall, and asia-southeastl) and minimize the IP addresses being used. What should you do?

- A. O 1- Configure a Private NAT gateway instance in us-westl (172.16.1.0/24), europe-centrall (172.16.2.0 /24), and asia-southeastl (172.16.3.0/24).
  2. Add the VPC as a spoke and configure an export include policy on the VPC spoke to advertise only the NAT subnets 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 to the hub.
  3. Enable global dynamic to allow resources in us-westl, us-centrall, and asia-southeastl to reach the on- premises location through us-east4.
- B. Q 1. Configure a Private NAT gateway instance in us-east4 (192.168.1.0/24).
  2. Add the VPC as a spoke and configure an export include policy on the VPC spoke to advertise 192.168.1.0/24 to the hub.
  3. Enable global dynamic routing to allow resources in us-westl, us-centrall and asia-southeast l to reach the on-premises location through us-east 4.
- C. Q 1. Configure a Private NAT gateway instance in us-westl (192.168.1.0/24), europe-centrall (192.168.2.0/24), and asia-southeastl (192.168.3.0/24).
  2. Add the VPC as a spoke and configure an export exclude policy on the VPC spoke to advertise only the NAT subnets 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 to the hub.
  3. Enable global dynamic routing to allow resources in us-westl, us-centrall, and asia-southeastl to reach the on-premises location through us-east4.
- D. O 1. Configure a Private NAT gateway and NAT subnet in us-westl (192.168.1.0/24), europe-centrall (192.168.2.0/24) and asia-southeastl (192.168.3.0/24).
  2. Add the VPC as a spoke and configure an export include policy to advertise only 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 to the hub.
  3. Enable global dynamic routing to allow resources in us-westl, us-centrall and asia-southeastl to reach the on-premises location through us-east4.

Answer: B

Explanation:
The key requirements are: limited IP space (192.168.0.0/20), reaching on-premises (172.16.0.0/16) from multiple Google Cloud regions (us-west1, europe-central1, asia-southeast1), and minimizing IP addresses used. The Cloud Interconnect connection to on-premises is in us-east4.
Minimize IP addresses and centralized NAT: Since all traffic to on-premises will traverse the Cloud Interconnect in us-east4, it's most efficient to configure a single Private NAT gateway instance in us-east4.
This allows resources from other regions to egress to on-premises through this single NAT gateway, using a minimal NAT subnet (192.168.1.0/24 in this case), thus conserving the limited 192.168.0.0/20 IP space.
Network Connectivity Center Spoke Export Policy: The VPC spoke needs to advertise the NAT subnet to the Network Connectivity Center hub. An export include policy is used to specify which routes (in this case, the 192.168.1.0/24 NAT subnet) should be advertised to the hub.
Global Dynamic Routing: To allow resources in us-west1, europe-central1, and asia-southeast1 to reach the on-premises location through the us-east4 Cloud Interconnect and NAT gateway, the VPC containing these resources (the spoke VPC) must have global dynamic routing enabled. This ensures that routes learned in one region (like the on-premises routes via us-east4) are available to VMs in all other regions of that VPC.
Options A and B configure Private NAT gateways in multiple regions, which consumes more IP addresses than necessary given that the Cloud Interconnect is only in us-east4. Option D uses 172.16.x.x for NAT subnets, which clashes with the on-premises IP range and the requirement to use the 192.168.0.0/20 space for cloud.

Exact Extract:
"Private NAT allows instances with private IP addresses in one VPC network to connect to on-premises or other cloud networks through a NAT IP address in a different region or network."
"To allow VMs in multiple regions to reach a central destination through a NAT gateway located in a specific region, you must configure global dynamic routing on the VPC network. This ensures that routes to the NAT gateway's subnet are propagated across all regions."
"When using Network Connectivity Center spokes, you can use export policies to control which routes are advertised from a spoke to the hub. An include policy specifies the exact prefixes to advertise."Reference:
Google Cloud Private NAT Documentation, Network Connectivity Center Documentation - Spoke policies, VPC Network Documentation - Dynamic routing mode

NEW QUESTION # 213
Your company runs an enterprise platform on-premises using virtual machines (VMS). Your internet customers have created tens of thousands of DNS domains panting to your public IP addresses allocated to the Vtvls Typically, your customers hard-code your IP addresses In their DNS records You are now planning to migrate the platform to Compute Engine and you want to use Bring your Own IP you want to minimize disruption to the Platform What Should you d0?

- A. Create a VPC With the same IP address range as your on-premises network Asson the IP addresses to the Compute Engine Instances.
- B. Verify ownership of your IP addresses. After the verification, Google Cloud advertises and provisions the IP prefix for you_ Assign the IP addresses to the Compute Engine Instances
- C. Create a VPC and request static external IP addresses from Google Cloud Assagn the IP addresses to the Compute Engine instances. Notify your customers of the new IP addresses so they can update their DNS
- D. Verify ownership of your IP addresses. Use live migration to import the prefix Assign the IP addresses to Compute Engine instances.

Answer: D

Explanation:
The correct answer is D because it allows you to use your own public IP addresses in Google Cloud without disrupting the platform or requiring your customers to update their DNS records. Option A is incorrect because it involves changing the IP addresses and notifying the customers, which can cause disruption and errors. Option B is incorrect because it does not use live migration, which is a feature that lets you control when Google starts advertising routes for your prefix. Option C is incorrect because it does not involve bringing your own IP addresses, but rather using Google-provided IP addresses.
Reference:
Bring your own IP addresses
Professional Cloud Network Engineer Exam Guide
Bring your own IP addresses (BYOIP) to Azure with Custom IP Prefix

NEW QUESTION # 214
Your organization is implementing a new security policy to control how firewall rules are applied to control flows between virtual machines (VMs). Using Google-recommended practices, you need to set up a firewall rule to enforce strict control of traffic between VM A and VM B.
You must ensure that communications flow only from VM A to VM B within the VPC, and no other communication paths are allowed. No other firewall rules exist in the VPC. Which firewall rule should you configure to allow only this communication path?

- A. Firewall rule direction: ingress
  Action: allow
  Target: VM A service account
  Source ranges: VM B service account and VM B source IP address
  Priority: 100
- B. Firewall rule direction: ingress
  Action: allow
  Target: specific VM A tag
  Source ranges: VM B tag and VM B source IP address
  Priority: 100
- C. Firewall rule direction: ingress
  Action: allow

Target: VM B service account
Source ranges: VM A service account
Priority: 1000

- D. Firewall rule direction: ingress
  Action: allow
  Target: specific VM B tag
  Source ranges: VM A tag and VM A source IP address
  Priority: 1000

Answer: B

NEW QUESTION # 215
You are creating a new GKE standard cluster. You need to configure the cluster to ensure that pods can reach other VMs in Google Cloud in the 192.168.0.0/24 subnet using the source IP of the GKE nodes. What should you do?

- A. Q Set a GKE pod IP address range that fits in 10.0.0.0/8. Do not configure the -disable-def ault-snat flag.
- B. Q Set a GKE pod IP address range that fits in 10.0.0.0/8. Configure the -disable-def ault-snat. flag.
- C. Q Set a GKE pod IP address range that does not fit in 10.0.0.0/8. Do not configure the -disable- default-snat flag.
- D. Q Set a GKE pod IP address range that does not fit in 10.0.0.0/8. Configure the -disable-default-snat flag.

Answer: B

Explanation:
By default, GKE uses SNAT (Source Network Address Translation) for pod egress traffic to destinations outside the cluster's IP ranges but within RFC 1918 private IP ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0
/16). This means that traffic from pods leaving the cluster for these private IP destinations will have their source IP address translated to the node's IP address.
To ensure pods can reach VMs in the 192.168.0.0/24 subnet using the source IP of the GKE nodes, you want the default SNAT behavior to apply to this destination. The default SNAT rule applies when the destination is an RFC 1918 address and the source is a pod IP that is not within the same RFC 1918 range as the destination (e.g., if your pods are in a 10.x.x.x range and the destination is 192.168.x.x).
Therefore, you should:
Set a GKE pod IP address range that fits in 10.0.0.0/8: This ensures that the pod IPs are within an RFC 1918 range different from 192.168.0.0/24.
Do NOT configure the --disable-default-snat flag: If you disable default SNAT, pods would use their own IP addresses as source IPs, which might not be routable to the 192.168.0.0/24 subnet unless specific routes are configured. The goal is to use the node's IP.
The combination of having pod IPs in a different RFC 1918 range and not disabling default SNAT ensures that GKE performs SNAT, making the node's IP the source for traffic destined for the 192.168.0.0/24 subnet.
Exact Extract:
"By default, GKE performs SNAT (Source Network Address Translation) for egress traffic from pods to destinations outside the cluster's IP address ranges but within the private IP address ranges defined in RFC
1918 (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). When SNAT occurs, the source IP address of the egress packets is the node's IP address instead of the pod's IP address."
"The --disable-default-snat flag, when used, disables this default SNAT behavior. If you want traffic to use the node's IP as the source when reaching internal RFC 1918 destinations, do not set this flag."Reference:
Google Kubernetes Engine Documentation - IP masquerade agent, Private IP addresses for GKE Pods and Services

NEW QUESTION # 216
Your organization has a hub and spoke architecture with VPC Network Peering, and hybrid connectivity is centralized at the hub. The Cloud Router in the hub VPC is advertising subnet routes, but the on-premises router does not appear to be receiving any subnet routes from the VPC spokes. You need to resolve this issue. What should you do?

- A. Create custom routes at the Cloud Router in the hub to advertise the subnets of the VPC spokes.
- B. Create custom routes at the Cloud Router in the spokes to advertise the subnets of the VPC spokes.
- C. Create custom learned routes at the Cloud Router in the hub to advertise the subnets of the VPC spokes.
- D. Create a BGP route policy at the Cloud Router, and ensure the subnets of the VPC spokes are being announced towards the on-premises environment.

Answer: D

Explanation:
Creating a BGP route policy at the Cloud Router ensures that the subnets of the VPC spokes are properly advertised to the on-premises environment. This allows the on-premises router to receive and use those routes. Without the correct BGP policies, route advertisement may not happen as expected.

NEW QUESTION # 217
.....

The language of our Professional-Cloud-Network-Engineer qualification test guide is simple. The learners may come from many social positions and their abilities to master our Professional-Cloud-Network-Engineer test materials are varied. Based on this consideration we apply the most simple and easy-to-be-understood language to help the learners no matter he or she is the students or the in-service staff, the novice or the experienced employee which have worked for many years. Professional-Cloud-Network-Engineer Certification guide use the simple language to explain the answers and detailed knowledge points to help pass the Professional-Cloud-Network-Engineer exam.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, ikanashop.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New Professional-Cloud-Network-Engineer dumps are available on Google Drive shared by PDFDumps: https://drive.google.com/open?id=1xEAu9AgD8hXL2hF3PW6j2bppMujR8zCR