100% Pass Guaranteed Free Professional-Cloud-Network-Engineer Exam Dumps Mar 07, 2023 [Q62-Q76

100% Pass Guaranteed Free Professional-Cloud-Network-Engineer Exam Dumps Mar 07, 2023

Verified & Latest Professional-Cloud-Network-Engineer Dump Q&As with Correct Answers

QUESTION 62

In order to provide subnet level isolation, you want to force instance-A in one subnet to route through a security appliance, called instance-B, in another subnet.

What should you do?

* Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with no tag.

* Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with a tag applied to instance-A.

* Delete the system-generated subnet route and create a specific route to instance-B with a tag applied to instance-A.

* Move instance-B to another VPC and, using multi-NIC, connect instance-B's interface to instance-A's network.

Configure the appropriate routes to force traffic through to instance-A.
Explanation/Reference:

QUESTION 63

You want to configure load balancing for an internet-facing, standard voice-over-IP (VOIP) application.

Which type of load balancer should you use?
* HTTP(S) load balancer
* Network load balancer
* Internal TCP/UDP load balancer
* TCP/SSL proxy load balancer

QUESTION 64

You need to give each member of your network operations team least-privilege access to create, modify, and delete Cloud Interconnect VLAN attachments.

What should you do?
* Assign each user the editor role.
* Assign each user the compute.networkAdmin role.
* Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get.
* Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get, compute.routers.create, compute.routers.get, compute.routers.update.
https://cloud.google.com/interconnect/docs/how-to/dedicated/creating-vlan-attachments

QUESTION 65

You have a Cloud Storage bucket in Google Cloud project XYZ. The bucket contains sensitive dat a. You need to design a solution to ensure that only instances belonging to VPCs under project XYZ can access the data stored in this Cloud Storage bucket. What should you do?
* Configure Private Google Access to privately access the Cloud Storage service using private IP addresses.
* Configure a VPC Service Controls perimeter around project XYZ, and include storage.googleapis.com as a restricted service in the service perimeter.
* Configure Cloud Storage with projectPrivate Access Control List (ACL) that gives permission to the project team based on their roles.
* Configure Private Service Connect to privately access Cloud Storage from all VPCs under project XYZ.

QUESTION 66

You created a new VPC for your development team. You want to allow access to the resources in this VPC via SSH only.

How should you configure your firewall rules?
* Create two firewall rules: one to block all traffic with priority 0, and another to allow port 22 with priority 1000.
* Create two firewall rules: one to block all traffic with priority 65536, and another to allow port 3389 with priority 1000.
* Create a single firewall rule to allow port 22 with priority 1000.
* Create a single firewall rule to allow port 3389 with priority 1000.

QUESTION 67

You want to create a service in GCP using IPv6.

What should you do?
* Create the instance with the designated IPv6 address.
* Configure a TCP Proxy with the designated IPv6 address.
* Configure a global load balancer with the designated IPv6 address.
* Configure an internal load balancer with the designated IPv6 address.
https://cloud.google.com/load-balancing/docs/load-balancing-overview mentions to use global load balancer for IPv6 termination.

QUESTION 68

You are configuring an HA VPN connection between your Virtual Private Cloud (VPC) and on-premises network. The VPN gateway is named VPN_GATEWAY_1. You need to restrict VPN tunnels created in the project to only connect to your on-premises VPN public IP address: 203.0.113.1/32. What should you do?
* Configure a firewall rule accepting 203.0.113.1/32, and set a target tag equal to VPN_GATEWAY_1.
* Configure the Resource Manager constraint constraints/compute.restrictVpnPeerIPs to use an allowList consisting of only the 203.0.113.1/32 address.
* Configure a Google Cloud Armor security policy, and create a policy rule to allow 203.0.113.1/32.
* Configure an access control list on the peer VPN gateway to deny all traffic except 203.0.113.1/32, and attach it to the primary external interface.

QUESTION 69

You have applications running in the us-west1 and us-east1 regions. You want to build a highly available VPN that provides 99.99% availability to connect your applications from your project to the cloud services provided by your partner’s project while minimizing the amount of infrastructure required. Your partner’s services are also in the us-west1 and us-east1 regions. You want to implement the simplest solution. What should you do?
* Create one Cloud Router and one HA VPN gateway in each region of your VPC and your partner’s VPC. Connect your VPN gateways to the partner’s gateways. Enable global dynamic routing in each VPC.
* Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC. Create one OpenVPN Access Server in each region of your partner’s VPC. Connect your VPN gateway to your partner’s servers.
* Create one OpenVPN Access Server in each region of your VPC and your partner’s VPC. Connect your servers to the partner’s servers.
* Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC and your partner’s VPC. Connect your VPN gateways to the partner’s gateways with a pair of tunnels. Enable global dynamic routing in each VPC.

QUESTION 70

You have a storage bucket that contains the following objects:

– folder-a/image-a-1.jpg

– folder-a/image-a-2.jpg

– folder-b/image-b-1.jpg

– folder-b/image-b-2.jpg

Cloud CDN is enabled on the storage bucket, and all four objects have been successfully cached.

You want to remove the cached copies of all the objects with the prefix folder-a, using the minimum number of commands.

What should you do?
* Add an appropriate lifecycle rule on the storage bucket.
* Issue a cache invalidation command with pattern /folder-a/*.
* Make sure that all the objects with prefix folder-a are not shared publicly.
* Disable Cloud CDN on the storage bucket. Wait 90 seconds. Re-enable Cloud CDN on the storage bucket.

QUESTION 71

Your company has recently expanded their EMEA-based operations into APAC. Globally distributed users report that their SMTP and IMAP services are slow. Your company requires end-to-end encryption, but you do not have access to the SSL certificates.

Which Google Cloud load balancer should you use?
* SSL proxy load balancer
* Network load balancer
* HTTPS load balancer
* TCP proxy load balancer

QUESTION 72

You want to deploy a VPN Gateway to connect your on-premises network to GCP. You are using a non BGP-capable on-premises VPN device. You want to minimize downtime and operational overhead when your network grows. The device supports only IKEv2, and you want to follow Google-recommended practices.

What should you do?
* * Create a Cloud VPN instance.* Create a policy-based VPN tunnel per subnet.* Configure the appropriate local and remote traffic selectors to match your local and remote networks.* Create the appropriate static routes.
* * Create a Cloud VPN instance.* Create a policy-based VPN tunnel.* Configure the appropriate local and remote traffic selectors to match your local and remote networks.* Configure the appropriate static routes.
* * Create a Cloud VPN instance.* Create a route-based VPN tunnel.* Configure the appropriate local and remote traffic selectors to match your local and remote networks.* Configure the appropriate static routes.
* * Create a Cloud VPN instance.* Create a route-based VPN tunnel.* Configure the appropriate local and remote traffic selectors to 0.0.0.0/0.* Configure the appropriate static routes.

QUESTION 73

Your company has provisioned 2000 virtual machines (VMs) in the private subnet of your Virtual Private Cloud (VPC) in the us-east1 region. You need to configure each VM to have a minimum of 128 TCP connections to a public repository so that users can download software updates and packages over the internet. You need to implement a Cloud NAT gateway so that the VMs are able to perform outbound NAT to the internet. You must ensure that all VMs can simultaneously connect to the public repository and download software updates and packages. Which two methods can you use to accomplish this? (Choose two.)
* Configure the NAT gateway in manual allocation mode, allocate 2 NAT IP addresses, and update the minimum number of ports per VM to 256.
* Create a second Cloud NAT gateway with the default minimum number of ports configured per VM to 64.
* Use the default Cloud NAT gateway’s NAT proxy to dynamically scale using a single NAT IP address.
* Use the default Cloud NAT gateway to automatically scale to the required number of NAT IP addresses, and update the minimum number of ports per VM to 128.
* Configure the NAT gateway in manual allocation mode, allocate 4 NAT IP addresses, and update the minimum number of ports per VM to 128.

QUESTION 74

You have configured a service on Google Cloud that connects to an on-premises service via a Dedicated Interconnect. Users are reporting recent connectivity issues. You need to determine whether the traffic is being dropped because of firewall rules or a routing decision. What should you do?

* Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.
* Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.
* Configure VPC Flow Logs. Review the logs by filtering on the source and destination.
* Configure a Compute Engine instance on the same VPC as the service running on Google Cloud to run a traceroute targeted at the on-premises service.

QUESTION 75

You have a storage bucket that contains two objects. Cloud CDN is enabled on the bucket, and both objects have been successfully cached. Now you want to make sure that one of the two objects will not be cached anymore, and will always be served to the internet directly from the origin.

What should you do?

* Ensure that the object you don’t want to be cached anymore is not shared publicly.
* Create a new storage bucket, and move the object you don’t want to be checked anymore inside it. Then edit the bucket setting and enable the privateattribute.
* Add an appropriate lifecycle rule on the storage bucket containing the two objects.
* Add a Cache-Controlentry with value private to the metadata of the object you don’t want to be cached anymore. Invalidate all the previously cached copies.
Explanation/Reference: https://developers.google.com/web/ilt/pwa/caching-files-with-service-worker

QUESTION 76

You have recently been put in charge of managing identity and access management for your organization. You have several projects and want to use scripting and automation wherever possible. You want to grant the editor role to a project member.

Which two methods can you use to accomplish this? (Choose two.)

* GetIamPolicy() via REST API
* setIamPolicy() via REST API
* gcloud pubsub add-iam-policy-binding Sprojectname –member user:Susername –role roles/editor
* gcloud projects add-iam-policy-binding Sprojectname –member user:Susername –role roles/editor
* Enter an email address in the Add members field, and select the desired role from the drop-down menu in the GCP Console.

Latest Professional-Cloud-Network-Engineer dumps - Instant Download PDF:
https://www.test4engine.com/Professional-Cloud-Network-Engineer_exam-latest-braindumps.html]