Vendor: Google

Exam Code:PROFESSIONAL-CLOUD-NETWORK-ENGINEER

Exam Name: Professional Cloud Network Engineer

Version: Demo

QUESTION 1

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?

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

B. 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.

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

D. 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.

Correct Answer: B

QUESTION 2

You need to create a GKE cluster in an existing VPC that is accessible from on-premises. You must meet the following requirements:

1.

IP ranges for pods and services must be as small as possible.

2.

The nodes and the master must not be reachable from the internet.

3.

You must be able to use kubectl commands from on-premises subnets to manage the cluster.

How should you create the GKE cluster?

A. Create a private cluster that uses VPC advanced routes. Set the pod and service ranges as /24. Set up a network proxy to access the master.

B. Create a VPC-native GKE cluster using GKE-managed IP ranges. Set the pod IP range as /21 and service IP range as /24. Set up a network proxy to access the master.

C. Create a VPC-native GKE cluster using user-managed IP ranges. Enable a GKE cluster network policy, set the pod and service ranges as /24. Set up a network proxy to access the master. Enable master authorized networks.

D. Create a VPC-native GKE cluster using user-managed IP ranges. Enable privateEndpoint on the cluster master. Set the pod and service ranges as /24. Set up a network proxy to access the master. Enable master authorized networks.

Correct Answer: C

Reference: https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips

---

QUESTION 3

You are using a 10-Gbps direct peering connection to Google together with the gsutil tool to upload files to Cloud Storage buckets from on-premises servers. The on-premises servers are 100 milliseconds away from the Google peering point. You notice that your uploads are not using the full 10-Gbps bandwidth available to you. You want to optimize the bandwidth utilization of the connection.

What should you do on your on-premises servers?

A. Tune TCP parameters on the on-premises servers.

B. Compress files using utilities like tar to reduce the size of data being sent.

C. Remove the -m flag from the gsutil command to enable single-threaded transfers.

D. Use the perfdiag parameter in your gsutil command to enable faster performance: gsutil perfdiaggs://[BUCKET_NAME].

Correct Answer: A

QUESTION 4

You create multiple Compute Engine virtual machine instances to be used at TFTP servers. Which type of load balancer should you use?

A. HTTP(S) load balancer

B. SSL proxy load balancer

C. TCP proxy load balancer

D. Network load balancer

Correct Answer: D

QUESTION 5

You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.

What should you do?

A. Configure VPC peering in a full mesh.

B. Alter the routing table to resolve the asymmetric route.

C. Create network tags to allow connectivity between all three VPCs.

D. Delete the legacy network and recreate it to allow transitive peering.

Correct Answer: A

QUESTION 6

You are adding steps to a working automation that uses a service account to authenticate. You need to drive the automation the ability to retrieve files from a Cloud Storage bucket. Your organization requires using the least privilege possible.

What should you do?

A. Grant the compute.instanceAdminto your user account.

B. Grant the iam.serviceAccountUserto your user account.

C. Grant the read-onlyprivilege to the service account for the Cloud Storage bucket.

D. Grant the cloud-platformprivilege to the service account for the Cloud Storage bucket.

Correct Answer: B

Reference: https://cloud.google.com/compute/docs/access/iam

QUESTION 7

You are creating an instance group and need to create a new health check for HTTP(s) load balancing.

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

A. Create a new health check using the gcloud command line tool.

B. Create a new health check using the VPC Network section in the GCP Console.

C. Create a new health check, or select an existing one, when you complete the load balancer\\'s backend configuration in the GCP Console.

D. Create a new legacy health check using the gcloudcommand line tool.

E. Create a new legacy health check using the Health checks section in the GCP Console.

Correct Answer: AE

Reference: https://cloud.google.com/load-balancing/docs/health-checks

---

QUESTION 8

You created a VPC network named Retail in auto mode. You want to create a VPC network named Distribution and peer it with the Retail VPC.

How should you configure the Distribution VPC?

A. Create the Distribution VPC in auto mode. Peer both the VPCs via network peering.

B. Create the Distribution VPC in custom mode. Use the CIDR range 10.0.0.0/9. Create the necessary subnets, and then peer them via network peering.

C. Create the Distribution VPC in custom mode. Use the CIDR range 10.128.0.0/9. Create the necessary subnets, and then peer them via network peering.

D. Rename the default VPC as "Distribution" and peer it via network peering.

Correct Answer: B

Reference: https://cloud.google.com/vpc/docs/using-vpc

QUESTION 9

You want to establish a dedicated connection to Google that can access Cloud SQL via a public IP address and that does not require a third-party service provider.

Which connection type should you choose?

A. Carrier Peering

B. Direct Peering

C. Dedicated Interconnect

D. Partner Interconnect

Correct Answer: B

Reference: https://cloud.google.com/interconnect/docs/how-to/direct-peering

---

QUESTION 10

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?

A. Ensure that the object you don\\'t want to be cached anymore is not shared publicly.

B. 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.

C. Add an appropriate lifecycle rule on the storage bucket containing the two objects.

D. Add a Cache-Control entry with value private to the metadata of the object you don\\'t want to be cached anymore. Invalidate all the previously cached copies.

Correct Answer: A

Reference: https://developers.google.com/web/ilt/pwa/caching-files-with-service-worker

---

QUESTION 11

You want to configure load balancing for an internet-facing, standard voice-over-IP (VOIP) application. Which type of load balancer should you use?

A. HTTP(S) load balancer

B. Network load balancer

C. Internal TCP/UDP load balancer

D. TCP/SSL proxy load balancer

Correct Answer: C

QUESTION 12

You are designing a shared VPC architecture. Your network and security team has strict controls over which routes are exposed between departments. Your Production and Staging departments can communicate with each other, but only via specific networks. You want to follow Google-recommended practices.

How should you design this topology?

A. Create 2 shared VPCs within the shared VPC Host Project, and enable VPC peering between them. Use firewall rules to filter access between the specific networks.

B. Create 2 shared VPCs within the shared VPC Host Project, and create a Cloud VPN/Cloud Router between them. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.

C. Create 2 shared VPCs within the shared VPC Service Project, and create a Cloud VPN/Cloud Router between them. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.

D. Create 1 VPC within the shared VPC Host Project, and share individual subnets with the Service Projects to filter access between the specific networks.

Correct Answer: D

Reference: https://cloud.google.com/vpc/docs/shared-vpc