## Question #:1

Your company has a security team that manages firewalls and SSL certificates. It also has a networking team that manages the networking resources. The networking team needs to be able to read firewall rules, but should not be able to create, modify, or delete them.

How should you set up permissions for the networking team?

A. Assign members of the networking team the compute.networkUser role.

B. Assign members of the networking team the compute.networkAdmin role.

C. Assign members of the networking team a custom role with only the compute.networks.* and the compute.firewalls.list permissions.

D. Assign members of the networking team the compute.networkViewer role, and add the compute.networks.use permission.

**Answer: B**

## Question #:2

You are designing a Google Kubernetes Engine (GKE) cluster for your organization. The current cluster size is expected to host 10 nodes, with 20 Pods per node and 150 services. Because of the migration of new services over the next 2 years, there is a planned growth for 100 nodes, 200 Pods per node, and 1500 services. You want to use VPC-native clusters with alias IP ranges, while minimizing address consumption.

How should you design this topology?

A. Create a subnet of size/25 with 2 secondary ranges of: /17 for Pods and /21 for Services. Create a VPC-native cluster and specify those ranges.

B. Create a subnet of size/28 with 2 secondary ranges of: /24 for Pods and /24 for Services. Create a VPC-native cluster and specify those ranges. When the services are ready to be deployed, resize the subnets.

C. Use gcloud container clusters create [CLUSTER NAME]--enable-ip-alias to create a VPC-native cluster.

D. Use gcloud container clusters create [CLUSTER NAME] to create a VPC-native cluster.

**Answer: B**

## Question #:3

You have an application running on Compute Engine that uses BigQuery to generate some results that are

stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.

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

    A.  Enable Private Google Access on all the subnets.

    B.  Enable Private Google Access on the VPC.

    C.  Enable Private Services Access on the VPC.

    D.  Create network peering between your VPC and BigQuery.

    E.  Create a Cloud NAT, and route the application traffic via NAT gateway.

**Answer: B E**

---

Question #:4

You are disabling DNSSEC for one of your Cloud DNS-managed zones. You removed the DS records from your zone file, waited for them to expire from the cache, and disabled DNSSEC for the zone. You receive reports that DNSSEC validating resolves are unable to resolve names in your zone.

What should you do?

    A.  Update the TTL for the zone.

    B.  Set the zone to the TRANSFER state.

    C.  Disable DNSSEC at your domain registar.

    D.  Transfer ownership of the domain to a new registar.

**Answer: C**

## Explanation

Before disabling DNSSEC for a managed zone you want to use, you must deactivate DNSSEC at your domain registrar to ensure that DNSSEC-validating resolvers can still resolve names in the zone.

---

Question #:5

You work for a multinational enterprise that is moving to GCP.

These are the cloud requirements:

• An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)

• Multiple regional offices in Europe and APAC

• Regional data processing is required in europe-west1 and australia-southeast1

• Centralized Network Administration Team

Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us-west1.

What should you do?

A. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

B. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

C. • Create 1 VPC in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in us-west1 subnet of the Host Project.• Attach NIC1 in us-west1 subnet of the Host Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

D. • Create 1 VPC in a Shared VPC Service Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in us-west1 subnet of the Service Project.• Attach NIC1 in us-west1 subnet of the Service Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

**Answer: A**

Question #:6

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.

**Answer: B**

Question #:7

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.instanceAdmin to your user account.

    B.  Grant the iam.serviceAccountUser to your user account.

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

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

**Answer: B**

Question #:8

You have ordered Dedicated Interconnect in the GCP Console and need to give the Letter of Authorization/Connecting Facility Assignment (LOA-CFA) to your cross-connect provider to complete the physical connection.

Which two actions can accomplish this? (Choose two.)

    A.  Open a Cloud Support ticket under the Cloud Interconnect category.

    B.  Download the LOA-CFA from the Hybrid Connectivity section of the GCP Console.

    C.  Run gcloud compute interconnects describe <interconnect>.

    D.  Check the email for the account of the NOC contact that you specified during the ordering process.

    E.  Contact your cross-connect provider and inform them that Google automatically sent the LOA/CFA to them via email, and to complete the connection.

**Answer: B D**

Question #:9

Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and