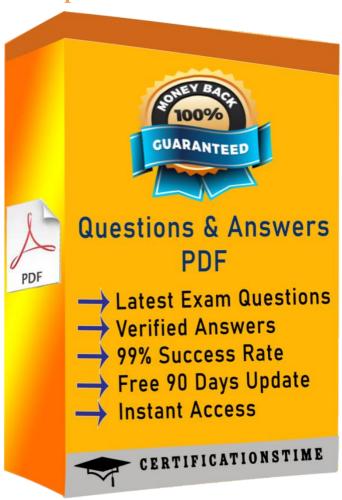# Exam Questions Professional-Cloud-Network-Engineer

Professional Cloud Network Engineer

https://certificationstime.com/

Question #:1

Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. You have recently engaged a traffic-scrubbing service and want to restrict your origin to allow connections only from the traffic-scrubbing service.

What should you do?

    A. Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.

    B. Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.

    C. Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.

    D. Create IPTables firewall rules that block all traffic except for the traffic-scrubbing service.

Answer: B

Question #:2

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 private attribute.

    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.

Answer: A

Question #:3

You have created an HTTP(S) load balanced service. You need to verify that your backend instances are responding properly.

How should you configure the health check?

    A. Set request-path to a specific URL used for health checking, and set proxy-header to PROXY_V1.

B. Set request-path to a specific URL used for health checking, and set host to include a custom host header that identifies the health check.

C. Set request-path to a specific URL used for health checking, and set response to a string that the backend service will always return in the response body.

D. Set proxy-header to the default value, and set host to include a custom host header that identifies the health check.

Answer: B

Question #:4

Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year. These are the assumptions for both GCP environments.

• Each organization has enabled full connectivity between all of its projects by using Shared VPC.

• Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic.

• There are no prefix overlaps between the two organizations.

• Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.

• Neither organization has Interconnects to their on-premises environment.

You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.

Which two steps should you take? (Choose two.)

A. Provision Cloud Interconnect to connect both organizations together.

B. Set up some variant of DNS forwarding and zone transfers in each organization.

C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.

D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.

E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

Answer: A D

Question #:5

Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to minimize operational overhead.

How should you design the topology?

A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.

B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.

C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.

D. Create a single project, and deploy specific firewall rules. Use network tags to isolate access between the departments.

Answer: A

Explanation

Use Shared VPC to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs. You can manage shared network resources, such as subnets, routes, and firewalls, from a central host project, enabling you to apply and enforce consistent network policies across the projects.

With Shared VPC and IAM controls, you can separate network administration from project administration. This separation helps you implement the principle of least privilege. For example, a centralized network team can administer the network without having any permissions into the participating projects. Similarly, the project admins can manage their project resources without any permissions to manipulate the shared network.

Question #:6

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.)

A. GetIamPolicy() via REST API

B. setIamPolicy() via REST API

C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor

D. gcloud projects add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor

E. Enter an email address in the Add members field, and select the desired role from the drop-down menu in the GCP Console.

Answer: D E

Question #:7

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 #:8

You want to use Cloud Interconnect to connect your on-premises network to a GCP VPC. You cannot meet Google at one of its point-of-presence (POP) locations, and your on-premises router cannot run a Border Gateway Protocol (BGP) configuration.

Which connectivity model should you use?

 A. Direct Peering

 B. Dedicated Interconnect

 C. Partner Interconnect with a layer 2 partner

 D. Partner Interconnect with a layer 3 partner

Answer: B

Question #:9

You want to use Partner Interconnect to connect your on-premises network with your VPC. You already have an Interconnect partner.

What should you first?

 A. Log in to your partner's portal and request the VLAN attachment there.

 B. Ask your Interconnect partner to provision a physical connection to Google.

 C. Create a Partner Interconnect type VLAN attachment in the GCP Console and retrieve the pairing key.

 D. Run gcloud compute interconnect attachments partner update <attachment> / -- region <region> --admin-enabled.

Answer: B

Question #:10

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?

 A. SSL proxy load balancer

B. Network load balancer

C. HTTPS load balancer

D. TCP proxy load balancer

Answer: A

For the Full Access Visit:

https://certificationstime.com/updated/professional-cloud-network-engineer-exam-dumps-pdf/

https://certificationstime.com/updated/professional-cloud-network-engineer-exam-dumps-pdf/