[Q45-Q67 Latest Professional-Cloud-Network-Engineer Exam with Accurate Google Cloud Certified - Professional Cloud Network Engineer PDF Questions [Mar 06, 2023

[Mar 06, 2023] Latest Professional-Cloud-Network-Engineer Exam with Accurate Google Cloud Certified - Professional Cloud Network Engineer PDF Questions

Practice To Professional-Cloud-Network-Engineer - Dumpleader Remarkable Practice On your Google Cloud Certified - Professional Cloud Network Engineer Exam

Manage & Monitor Network Operations

In this part of the exam content, the students should be able to log and monitor with the use of GCP Console or Stackdriver. They must have competence in the management and maintenance of security, which includes firewalls and diagnosing & resolving IAM problems. Besides that, they need to be able to deal with the following objective: - Maintain & Troubleshoot Connectivity Issues: It includes the identification of traffic flow topology, redirecting and draining of traffic flows, and cross-connect hand-off for interconnect. It also measures one's knowledge of the monitoring of egress and ingress traffic with the use of flow logs as well as monitoring firewall logs. This section will also evaluate the learners' skills in troubleshooting and managing VPNs and troubleshooting peering issues with Cloud Router BGP.

The applicants should also demonstrate competence in troubleshooting, monitoring, and maintaining traffic flow and latency, which include routing issues, network latency testing & throughput, and tracing traffic flow.

Exam Details and Topics

As for the qualifying exam, you need to know that it can only be taken in the English language, and the candidates have two hours for its completion. The question formats of the test include multiple choice and multiple select. The cost for taking the Professional Cloud Network Engineer certification exam is $200. You can choose to sit for it as an online proctored or an on-site proctored option.

NEW QUESTION 45

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.)
* Provision Cloud Interconnect to connect both organizations together.
* Set up some variant of DNS forwarding and zone transfers in each organization.
* Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
* Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
* Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC

NEW QUESTION 46

Your organization requires that metrics from all applications be retained for 5 years for future analysis in possible legal proceedings.
Which approach should you use?
* Configure Stackdriver Monitoring for all Projects, and export to BigQuery.
* Configure Stackdriver Monitoring for all Projects with the default retention policies.
* Configure Stackdriver Monitoring for all Projects, and export to Google Cloud Storage.
* Grant the security team access to the logs in each Project.
B and D can be quickly ruled out because none of them is good solution for the requirements

“retained for 5 years”

Between A and C, the different is where to store, BigQuery or Cloud Storage. Since the main concern is extended storing period, C (Correct Answer) is better answer, and the “retained for 5 years for future analysis” further qualifies it, for example, using Coldline storage class.

With regards of BigQuery, while it is also a low-cost storage, but the main purpose is for analysis.

Also, logs in Cloud Storage is easy to transport to BigQuery whenever needed.

NEW QUESTION 47

You are creating a new application and require access to Cloud SQL from VPC instances without public IP addresses.

Which two actions should you take? (Choose two.)
* Activate the Service Networking API in your project.
* Activate the Cloud Datastore API in your project.
* Create a private connection to a service producer.
* Create a custom static route to allow the traffic to reach the Cloud SQL API.
* Enable Private Google Access.
https://cloud.google.com/sql/docs/mysql/configure-private-services-access#console_1 C: If you are using private IP for any of your Cloud SQL instances, you only need to configure private services access one time for every Google Cloud project that has or needs to connect to a Cloud SQL instance. If your Google Cloud project has a Cloud SQL instance, you can either configure it yourself or let Cloud SQL do it for you to use private IP. Cloud SQL configures private services access for you when all the conditions below are true: https://cloud.google.com/sql/docs/postgres/configure-private-services-access#before_you_begin E: You can enable Private Google access on a subnet level and any VMs on that subnet can access Google APIs by using their internal IP address. https://cloud.google.com/vpc/docs/configure-private-google-access

NEW QUESTION 48

You work for a university that is migrating to Google Cloud.

These are the cloud requirements:

On-premises connectivity with 10 Gbps

Lowest latency access to the cloud

Centralized Networking Administration Team

New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.

What should you do?
* Use Shared VPC, and deploy the VLAN attachments and Dedicated Interconnect in the host project.
* Use Shared VPC, and deploy the VLAN attachments in the service projects. Connect the VLAN attachment to the Shared VPC’s host project.
* Use standalone projects, and deploy the VLAN attachments in the individual projects. Connect the VLAN attachment to the standalone projects’ Dedicated Interconnects.
* Use standalone projects and deploy the VLAN attachments and Dedicated Interconnects in each of the individual projects.

NEW QUESTION 49

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?
* Assign members of the networking team the compute.networkUser role.
* Assign members of the networking team the compute.networkAdmin role.
* Assign members of the networking team a custom role with only the compute.networks.* and the compute.firewalls.list permissions.
* Assign members of the networking team the compute.networkViewer role, and add the compute.networks.use permission.
https://cloud.google.com/compute/docs/access/iam

NEW QUESTION 50

You have two Google Cloud projects in a perimeter to prevent data exfiltration. You need to move a third project inside the perimeter; however, the move could negatively impact the existing environment. You need to validate the impact of the change.
What should you do?
* Enable Firewall Rules Logging inside the third project.
* Modify the existing VPC Service Controls policy to include the new project in dry run mode.
* Monitor the Resource Manager audit logs inside the perimeter.
* Enable VPC Flow Logs inside the third project, and monitor the logs for negative impact.

NEW QUESTION 51

You want to configure a NAT to perform address translation between your on-premises network blocks and GCP.

Which NAT solution should you use?
* Cloud NAT
* An instance with IP forwarding enabled

* An instance configured with iptables DNAT rules
* An instance configured with iptables SNAT rules

NEW QUESTION 52

You are designing the network architecture for your organization. Your organization has three developer teams: Web, App, and Database. All of the developer teams require access to Compute Engine instances to perform their critical tasks. You are part of a small network and security team that needs to provide network access to the developers. You need to maintain centralized control over network resources, including subnets, routes, and firewalls. You want to minimize operational overhead. How should you design this topology?
* Configure a host project with a Shared VPC. Create service projects for Web, App, and Database.
* Configure one VPC for Web, one VPC for App, and one VPC for Database. Configure HA VPN between each VPC.
* Configure three Shared VPC host projects, each with a service project: one for Web, one for App, and one for Database.
* Configure one VPC for Web, one VPC for App, and one VPC for Database. Use VPC Network Peering to connect all VPCs in a full mesh.

NEW QUESTION 53

You are a admin at XYZ organization. Few of your team members need to use BigQuery Data Transfer Service for Amazon S3 . They want to automatically schedule and manage recurring load jobs from Amazon S3 into BigQuery, they want to run the transfer job every week. They have, Amazon S3 URI for the source data, access key ID , secret access key and Read permission on the data source . What necessary permissions are required for the transfer job creators in BigQuery .
* bigquery.transfers.update and bigquery.datasets.update
* bigquery.transfers.update and bigquery.transfers.get
* bigquery.transfer.get and bigquery.data.sets.update
* bigquery.jobs.create and bigquery.transfers.get
Option A is the correct choice because bigquery.transfers.update permissions is needed to create the transfer and bigquery.datasets.update permissions is needed on the target dataset .Also The bigquery.admin predefined Cloud IAM role includes bigquery.transfers.update and bigquery.datasets.update permissions .

Option B is Incorrect because , it is not the required permission for transfer job creators.

Option C and Option D are Incorrect because , they are not the required permission for transfer job creators.

NEW QUESTION 54

You need to configure a Google Kubernetes Engine (GKE) cluster. The initial deployment should have 5 nodes with the potential to scale to 10 nodes. The maximum number of Pods per node is 8. The number of services could grow from 100 to up to 1024. How should you design the IP schema to optimally meet this requirement?
* Configure a /28 primary IP address range for the node IP addresses. Configure a (25 secondary IP range for the Pods. Configure a /22 secondary IP range for the Services.
* Configure a /28 primary IP address range for the node IP addresses. Configure a /25 secondary IP range for the Pods. Configure a /21 secondary IP range for the Services.
* Configure a /28 primary IP address range for the node IP addresses. Configure a /28 secondary IP range for the Pods. Configure a /21 secondary IP range for the Services.
* Configure a /28 primary IP address range for the node IP addresses. Configure a /24 secondary IP range for the Pads. Configure a /22 secondary IP range for the Services.

NEW QUESTION 55

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.

NEW QUESTION 56

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.)
* Provision Cloud Interconnect to connect both organizations together.
* Set up some variant of DNS forwarding and zone transfers in each organization.
* Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
* Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
* Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.
https://cloud.google.com/dns/docs/best-practices

NEW QUESTION 57

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.

NEW QUESTION 58

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?
* 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.
* 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.
* 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.
* 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.

NEW QUESTION 59

You recently deployed two network virtual appliances in us-central1. Your network appliances provide connectivity to your on-premises network, 10.0.0.0/8. You need to configure the routing for your Virtual Private Cloud (VPC). Your design must meet the following requirements:

All access to your on-premises network must go through the network virtual appliances.

Allow on-premises access in the event of a single network virtual appliance failure.

Both network virtual appliances must be used simultaneously.

Which method should you use to accomplish this?
* Configure two routes for 10.0.0.0/8 with different priorities, each pointing to separate network virtual appliances.
* Configure an internal HTTP(S) load balancer with the two network virtual appliances as backends. Configure a route for 10.0.0.0/8 with the internal HTTP(S) load balancer as the next hop.
* Configure a network load balancer for the two network virtual appliances. Configure a route for 10.0.0.0/8 with the network load balancer as the next hop.
* Configure an internal TCP/UDP load balancer with the two network virtual appliances as backends. Configure a route for 10.0.0.0/8 with the internal load balancer as the next hop.

NEW QUESTION 60

You need to enable Cloud CDN for all the objects inside a storage bucket. You want to ensure that all the objects in the storage bucket can be served by the CDN.

What should you do in the GCP Console?
* Create a new cloud storage bucket, and then enable Cloud CDN on it.
* Create a new TCP load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
* Create a new SSL proxy load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
* Create a new HTTP load balancer, select the storage bucket as a backend, enable Cloud CDN on the backend, and make sure each object inside the storage bucket is shared publicly.

NEW QUESTION 61

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?
* Direct Peering
* Dedicated Interconnect
* Partner Interconnect with a layer 2 partner
* Partner Interconnect with a layer 3 partner
Reference:

https://cloud.google.com/interconnect/docs/support/faq

NEW QUESTION 62

Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from on-premises locations using Cloud Interconnect connections. Your company must be able to send traffic to Cloud Storage only through the Interconnect links while accessing other Google APIs and services over the public internet. What should you do?
* Use the default public domains for all Google APIs and services.
* Use Private Service Connect to access Cloud Storage, and use the default public domains for all other Google APIs and services.
* Use Private Google Access, with restricted.googleapis.com virtual IP addresses for Cloud Storage and private.googleapis.com for all other Google APIs and services.
* Use Private Google Access, with private.googleapis.com virtual IP addresses for Cloud Storage and restricted.googleapis.com virtual IP addresses for all other Google APIs and services.

NEW QUESTION 63

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.
Explanation/Reference: https://cloud.google.com/iam/docs/granting-changing-revoking-access

NEW QUESTION 64

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?
* Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.
* Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.
* Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.

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

NEW QUESTION 65

One instance in your VPC is configured to run with a private IP address only. You want to ensure that even if this instance is deleted, its current private IP address will not be automatically assigned to a different instance.

In the GCP Console, what should you do?
* Assign a public IP address to the instance.
* Assign a new reserved internal IP address to the instance.
* Change the instance’s current internal IP address to static.
* Add custom metadata to the instance with key internal-address and value reserved.

NEW QUESTION 66

You need to configure a static route to an on-premises resource behind a Cloud VPN gateway that is configured for policy-based routing using the gcloud command.

Which next hop should you choose?
* The default internet gateway
* The IP address of the Cloud VPN gateway
* The name and region of the Cloud VPN tunnel
* The IP address of the instance on the remote side of the VPN tunnel

Reference:

https://cloud.google.com/vpn/docs/how-to/creating-static-vpns

NEW QUESTION 67

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?
* Log in to your partner’s portal and request the VLAN attachment there.
* Ask your Interconnect partner to provision a physical connection to Google.
* Create a Partner Interconnect type VLAN attachment in the GCP Console and retrieve the pairing key.
* Run gcloud compute interconnect attachments partner update <attachment> / — region <region> –admin-enabled.

Reference:

https://cloudplatform.googleblog.com/2018/06/Partner-Interconnect-now-generally-available.html

Exam Questions and Answers for Professional-Cloud-Network-Engineer Study Guide Questions and Answers!:

https://www.dumpleader.com/Professional-Cloud-Network-Engineer_exam.html]