Free Questions for Professional-Cloud-Network-Engineer by actualtestdumps

Shared by Oliver on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are responsible for designing a new connectivity solution for your organization's enterprise network to access and use Google Workspace. You have an existing Shared VPC with Compute Engine instances in us-west1. Currently, you access Google Workspace via your service provider's internet access. You want to set up a direct connection between your network and Google. What should you do?

Options:

A- Order a Dedicated Interconnect connection in the same metropolitan area. Create a VLAN attachment, a Cloud Router in us-west1, and a Border Gateway Protocol (BGP) session between your Cloud Router and your router.

B- Order a Direct Peering connection in the same metropolitan area. Configure a Border Gateway Protocol (BGP) session between Google and your router.

C- Configure HA VPN in us-west1. Configure a Border Gateway Protocol (BGP) session between your Cloud Router and your on-premises data center.

D- Order a Carrier Peering connection in the same metropolitan area. Configure a Border Gateway Protocol (BGP) session between Google and your router.

Answer:

B

Question 2

Question Type: MultipleChoice

You need to define an address plan for a future new Google Kubernetes Engine (GKE) cluster in your Virtual Private Cloud (VPC). This will be a VPC-native cluster, and the default Pod IP range allocation will be used. You must pre-provision all the needed VPC subnets and their respective IP address ranges before cluster creation. The cluster will initially have a single node, but it will be scaled to a maximum of three nodes if necessary. You want to allocate the minimum number of Pod IP addresses. Which subnet mask should you use for the Pod IP address range?

Options:

A- /21

B- /22

C- /23

D- /25

Answer:

A

Question 3

Question Type: MultipleChoice

You are configuring a new HTTP application that will be exposed externally behind both IPv4 and IPv6 virtual IP addresses, using ports 80, 8080, and 443. You will have backends in two regions: us-west1 and us-east1. You want to serve the content with the lowest-possible latency while ensuring high availability and autoscaling, and create native content-based rules using the HTTP hostname and request path. The IP addresses of the clients that connect to the load balancer need to be visible to the backends. Which configuration should you use?

Options:

A- Use Network Load Balancing

B- Use TCP Proxy Load Balancing with PROXY protocol enabled

C- Use External HTTP(S) Load Balancing with URL Maps and custom headers

D- Use External HTTP(S) Load Balancing with URL Maps and an X-Forwarded-For header

Answer:

D

Question 4

Question Type: MultipleChoice

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?

Options:

A- Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.

B- Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.

C- Configure VPC Flow Logs. Review the logs by filtering on the source and destination.

D- 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.

Answer:

B

Question 5

Question Type: MultipleChoice

Your organization is implementing a new security policy to control how firewall rules are applied to control flows between virtual machines (VMs). Using Google-recommended practices, you need to set up a firewall rule to enforce strict control of traffic between VM A and VM B. You must ensure that communications flow only from VM A to VM B within the VPC, and no other communication paths are allowed. No other firewall rules exist in the VPC. Which firewall rule should you configure to allow only this communication path?

Options:

A- Firewall rule direction: ingress
Action: allow
Target: VM B service account
Source ranges: VM A service account
Priority: 1000

B- Firewall rule direction: ingress
Action: allow
Target: specific VM B tag
Source ranges: VM A tag and VM A source IP address
Priority: 1000

C- Firewall rule direction: ingress
Action: allow
Target: VM A service account

Source ranges: VM B service account and VM B source IP address
Priority: 100

D- Firewall rule direction: ingress
Action: allow
Target: specific VM A tag
Source ranges: VM B tag and VM B source IP address
Priority: 100

Answer:

D

Question 6

Question Type: **MultipleChoice**

Your organization uses a Shared VPC architecture with a host project and three service projects. You have Compute Engine instances that reside in the service projects. You have critical workloads in your on-premises data center. You need to ensure that the Google Cloud instances can resolve on-premises hostnames via the Dedicated Interconnect you deployed to establish hybrid connectivity. What should you do?

Options:

A- Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the private zone to the on-premises DNS servers.
In your Cloud Router, add a custom route advertisement for the IP 35.199.192.0/19 to the on-premises environment.

B- Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the Private zone to the on-premises DNS servers.
In your Cloud Router, add a custom route advertisement for the IP 169.254 169.254 to the on-premises environment.

C- Configure a Cloud DNS private zone in the host project of the Shared VPC.
Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project
In your Cloud Router, add a custom route advertisement for the IP 169.254 169 254 to the on-premises environment.

D- Configure a Cloud DNS private zone in the host project of the Shared VPC.
Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project.
Configure a DNS policy in the Shared VPC to allow inbound query forwarding with your on-premises DNS server as the alternative DNS server.

Answer:

D

Question 7

Question Type: MultipleChoice

Your organization has a Google Cloud Virtual Private Cloud (VPC) with subnets in us-east1, us-west4, and europe-west4 that use the default VPC configuration. Employees in a branch office in Europe need to access the resources in the VPC using HA VPN. You configured the HA VPN associated with the Google Cloud VPC for your organization with a Cloud Router deployed in europe-west4. You need to ensure that the users in the branch office can quickly and easily access all resources in the VPC. What should you do?

Options:

A- Create custom advertised routes for each subnet.

B- Configure each subnet's VPN connections to use Cloud VPN to connect to the branch office.

C- Configure the VPC dynamic routing mode to Global.

D- Set the advertised routes to Global for the Cloud Router.

Answer:

C

Question 8

Question Type: MultipleChoice

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?

Options:

A- Use the default public domains for all Google APIs and services.

B- Use Private Service Connect to access Cloud Storage, and use the default public domains for all other Google APIs and services.

C- 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.

D- 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.

Answer:

B

Question 9

Question Type: **MultipleChoice**

You configured Cloud VPN with dynamic routing via Border Gateway Protocol (BGP). You added a custom route to advertise a network that is reachable over the VPN tunnel. However, the on-premises clients still cannot reach the network over the VPN tunnel. You need to examine the logs in Cloud Logging to confirm that the appropriate routers are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

Options:

A- resource.type= "gce_router"

B- resource.type= "gce_network_region"

C- resource.type= "vpn_tunnel"

D- resource.type= "vpn_gateway"

Answer:

C