Google Professional-Cloud-Network-Engineer Practice Questions

Shared by Pugh on 24-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Your organization is migrating workloads from AWS to Google Cloud. Because a particularly critical workload will take longer to migrate, you need to set up Google Cloud CDN and point it to the existing application at AWS. What should you do?

Options:

A- Create a hybrid NEG that points to the existing IP of the application.
* Map the NEG to a passthrough Network Load Balancer as a target pool.
* Enable Cloud CDN on the target pool.
B- Create an internet NEG that points to the existing FQDN of the application.
* Map the NEG to an Application Load Balancer as a backend service.
* Enable Cloud CDN on the backend service.
C- Create a hybrid NEG that points to the existing IP of the application.
* Map the NEG to an Application Load Balancer as a backend service.
* Enable Cloud CDN on the backend service.
D- Create an internet NEG that points to the existing FQDN of the application.
* Map the NEG to a passthrough Network Load Balancer as a backend service.
* Enable Cloud CDN on the backend service.

Answer:

B

Explanation:

To configure Cloud CDN for an application hosted outside of Google Cloud (e.g., in AWS), you need to use an internet network endpoint group (NEG). An internet NEG allows you to point to external endpoints using their FQDN or IP address. Cloud CDN works with external HTTP(S) Load Balancers, and you enable CDN on the backend service associated with the load balancer. A Network Load Balancer (passthrough) does not support Cloud CDN.

Exact Extract:

'To enable Cloud CDN for content hosted outside of Google Cloud, you must use an external HTTP(S) Load Balancer with an internet network endpoint group (NEG).'

'An internet NEG specifies one or more external endpoints that can be reached by an external HTTP(S) Load Balancer. You can specify endpoints using an IP address and port, or a fully qualified domain name (FQDN) and port.'

Question 2

Question Type: MultipleChoice

Your organization's security policy requires that all internet-bound traffic return to your on-premises data center through HA VPN tunnels before egressing to the internet, while allowing virtual machines (VMs) to leverage private Google APIs using private virtual IP addresses 199.36.153.4/30. You need to configure the routes to enable these traffic flows. What should you do?

Options:

A- Configure a custom route 0.0.0.0/0 with a priority of 500 whose next hop is the default internet gateway. Configure another custom route 199.36.153.4/30 with priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.
B- Configure a custom route 0.0.0.0/0 with a priority of 1000 whose next hop is the internet gateway. Configure another custom route 199.36.153.4/30 with a priority of 500 whose next hop is the VPN tunnel back to the on-premises data center.
C- Announce a 0.0.0.0/0 route from your on-premises router with a MED of 1000. Configure a custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the default internet gateway.
D- Announce a 0.0.0.0/0 route from your on-premises router with a MED of 500. Configure another custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the VPN tunnel back to the on-
premises data center.

Answer:

A

Question 3

Question Type: MultipleChoice

You are designing a hybrid cloud environment. Your Google Cloud environment is interconnected with your on-premises network using HA VPN and Cloud Router in a central transit hub VPC. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88. You need to ensure that your Compute Engine resources in multiple spoke VPCs can resolve on-premises private hostnames using the domain corp.altostrat.com while also resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

Options:

A- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Configure VPC peering in the spoke VPCs to peer with the hub VPC.
B- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Associate the zone with the hub VPC. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke PCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
C- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Create a hub-and-spoke VPN deployment in each spoke VPC to connect back to the on-premises network directly.
D- Create a private forwarding zone in Cloud DNS for 'corp altostrat.com' called corp-altostrat-com that points to 192. 168.20.88. Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
Sat a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Create a hub and spoke VPN deployment in each spoke VPC to connect back to the hub VPC.

Answer:

A

Question 4

Question Type: MultipleChoice

You are designing a new application that has backends internally exposed on port 800. The application will be exposed externally using both IPv4 and IPv6 via TCP on port 700. You want to ensure high availability for this application. What should you do?

Options:

A- Create a network load balancer that used backend services containing one instance group with two instances.
B- Create a network load balancer that uses a target pool backend with two instances.
C- Create a TCP proxy that uses a zonal network endpoint group containing one instance.

D- Create a TCP proxy that uses backend services containing an instance group with two instances.

Answer:

D

Question 5

Question Type: MultipleChoice

You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.

Which session affinity should you Select?

Options:

A- None
B- Client IP
C- Client IP and protocol
D- Client IP, port and protocol

Answer:

B

Question 6

Question Type: MultipleChoice

You are designing a hybrid cloud environment for your organization. Your Google Cloud environment is interconnected with your on-premises network using Cloud HA VPN and Cloud Router. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88 and is protected by a firewall, and your Compute Engine resources are located at 10.204.0.0/24. Your Compute Engine resources need to resolve on-premises private hostnames using the domain corp.altostrat.com while still resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

Options:

A- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Configure your on-premises firewall to accept traffic from 10.204.0.0/24.
Set a custom route advertisement on the Cloud Router for 10.204.0.0/24
B- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168 20.88.
Configure your on-premises firewall to accept traffic from 35.199.192.0/19
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
C- Create a private forwarding zone in Cloud DNS for 'corp .altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Configure your on-premises firewall to accept traffic from 10.204.0.0/24.
Modify the /etc/resolv conf file on your Compute Engine instances to point to 192.168.20 88
D- Create a private zone in Cloud DNS for 'corp altostrat.com' called corp-altostrat-com.
Configure DNS Server Policies and create a policy with Alternate DNS servers to 192.168.20.88.
Configure your on-premises firewall to accept traffic from 35.199.192.0/19.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

Answer:

D

Question 7

Question Type: MultipleChoice

You are configuring the final elements of a migration effort where resources have been moved from on-premises to Google Cloud. While reviewing the deployed architecture, you noticed that DNS resolution is failing when queries are being sent to the on-premises environment. You log in to a Compute Engine instance, try to resolve an on-premises hostname, and the query fails. DNS queries are not arriving at the on-premises DNS server. You need to use managed services to reconfigure Cloud DNS to resolve the DNS error. What should you do?

Options:

A- Validate that the Compute Engine instances are using the Metadata Service IP address as their resolver. Configure an outbound forwarding zone for the on-premises domain pointing to the on-premises DNS server. Configure Cloud Router to advertise the Cloud DNS proxy range to the on-premises network.
B- Validate that there is network connectivity to the on-premises environment and that the Compute Engine instances can reach other on-premises resources. If errors persist, remove the VPC Network Peerings and recreate the peerings after validating the routes.
C- Review the existing Cloud DNS zones, and validate that there is a route in the VPC directing traffic destined to the IP address of the DNS servers. Recreate the existing DNS forwarding zones to forward all queries to the on-premises DNS servers.

D- Ensure that the operating systems of the Compute Engine instances are configured to send DNS queries to the on-premises DNS servers directly.

Answer:

A

Explanation:

To resolve DNS resolution issues for on-premises domains from Google Cloud, you should use Cloud DNS outbound forwarding zones. This setup forwards DNS requests for specific domains to on-premises DNS servers. Cloud Router is needed to advertise the range for the DNS proxy service back to the on-premises environment, ensuring that DNS queries from Compute Engine instances reach the on-premises DNS servers.

Question 8

Question Type: MultipleChoice

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?

Options:

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

Explanation:

https://cloud.google.com/vpc/docs/vpc#ip-ranges